

**E L E M E N T A R Y**

---

**T H E O R Y   O F**

---

**E Q U A T I O N S**

SAMUEL BOROFSKY, *Brooklyn College*

NEW YORK

**T H E   M A C M I L L A N   C O M P A N Y**

**Printed in the United States of America**

## P R E F A C E

This presentation of the elementary theory of equations has the aim not only of acquainting the student with some facts concerning the roots of algebraic equations and methods for obtaining them but also of introducing him gently to some of the concepts of present-day algebra. Therefore, the notions of field and polynomial over a field are used throughout. For the sake of concreteness, however, only fields which are subfields of the complex number system are considered, although so far as possible the material is presented so as to be applicable to other fields. It is hoped that in this way the text will serve as a bridge between the ideas of elementary algebra which the student has already encountered and the more abstract ideas of modern algebra.

Although it is desirable from the algebraic standpoint to define polynomials as elements of certain rings rather than as functions, the author has adopted the latter approach since he has found the former too abstract for the average beginner.

No experience with the calculus is presupposed. Derivatives and their properties are required only for polynomials and results which depend upon them are derived purely algebraically. Some trigonometry and plane analytic geometry are required in parts of Chapter 8 and 9, but no demands beyond these are made upon the student's previous mathematical experience.

Since the method of mathematical induction is used frequently, it is discussed at length in an Appendix.

The first eight chapters contain sufficient material for a brief course. Chapter 9 depends only upon 1, 2, 3, 8; Chapter 10 only upon 1, 2, 3, and the first two sections of 5; Chapter 11 only upon 1, 2, 3. Chapter 12 requires only 1, while 13 requires 1, 2, 12. Chapters 1, 2, 3, 12, 13 suffice for 14, except that the last three sections of 14 require in addition the first three sections of 11.





# **C O N T E N T S**

## **1. THE COMPLEX NUMBER SYSTEM**

1. Introduction	1
2. Complex numbers	1
3. Real and imaginary complex numbers	4
4. Modulus	7
5. Polar form	10
6. Roots of complex numbers	12

## **2. POLYNOMIALS IN ONE VARIABLE**

1. Definition of polynomial	15
2. Sums and products of polynomials	16
3. Factor theorem	16
4. Uniqueness of representation	17
5. Number fields	21
6. Division algorithm	23
7. Divisibility of polynomials	26
8. Highest common factor	27
9. Form for H.C.F.	29
10. Relatively prime polynomials	30
11. Irreducible polynomials	31
12. Factorization into primes	33
13. Factorization of integers	36

## **3. POLYNOMIALS IN THE COMPLEX DOMAIN**

1. Factorization into linear factors	39
2. Multiplicity of roots	40
3. Synthetic division	41
4. Relations between roots and coefficients	44
5. Transformations of the roots	48
6. Common roots	51

**4. DERIVATIVES AND MULTIPLE ROOTS**

1. Derivatives	54
2. Multiple roots	56
3. Expansions of polynomials	60
4. Taylor expansion	61

**5. POLYNOMIALS WITH REAL COEFFICIENTS**

1. Factorization	64
2. Rational roots	67
3. Conjugate square roots	70
4. Location principle	72
5. Sign for large values of $x$	74
6. Rolle's theorem	77
7. Monotoneity	79
8. Graphs	82

**6. THEOREMS OF BUDAN AND STURM**

1. Introduction	85
2. Variations in sign	85
3. Budan sequence	85
4. Budan's theorem	87
5. Roots exceeding a given number	92
6. Sturm sequence	96
7. Sturm's theorem	98
8. Roots exceeding a given number	101

**7. APPROXIMATIONS TO REAL ROOTS**

1. Introduction	103
2. Graphical approximation	103
3. Approximation by location principle	104
4. Determination of successive decimal places	105
5. Horner's method	105
6. Newton's method	108
7. Validity of Newton's method	110

**8. CUBIC AND QUARTIC EQUATIONS**

1. Solvability by radicals	114
2. Cardan's solution of cubic	115

3. Verification of the roots	117
4. Example	119
5. Discriminant of cubic	122
6. Cubics with three real roots	125
7. Ferrari's solution of quartic	128
8. Roots of resolvent cubic	129

## 9. RULER AND COMPASS CONSTRUCTIONS

1. Definition of constructibility	132
2. Criterion for constructibility	133
3. Problem of trisecting an angle	138
4. Multiple square roots	138
5. Criterion for cubics	140
6. Impossibility of certain constructions	142
7. Criterion for quartics	146
8. Remarks on angle trisection	149
9. Remarks on regular polygons	151
10. Circle squaring	152

## 10. ALGEBRAIC NUMBER FIELDS

1. Numbers algebraic over a field	153
2. Extension of $\mathbb{C}$ field	155
3. Algebraic extensions	157
4. Adjunction to a field	159
5. Adjunction of algebraic numbers	160
6. Adjunction of radicals	164
7. Expressibility by radicals	166

## 11. SYMMETRIC POLYNOMIALS

1. Polynomials in several variables	170
2. Uniqueness of representation	172
3. Products of polynomials	175
4. Elementary symmetric polynomials	178
5. Some properties of symmetric polynomials	179
6. Fundamental theorem on symmetric polynomials	182
7. Weight	185

**12. DETERMINANTS**

1. Introduction	189
2. Definition of determinant	190
3. Expansion of a determinant	192
4. Cofactors	195
5. Expansion by columns	196
6. Interchange of rows and columns	197
7. Some properties of determinants	198
8. Product of determinants	204
9. Rank of matrix	206

**13. LINEAR EQUATIONS**

1. Linear dependence of constants	212
2. Criterion for linear dependence	214
3. Linear equations	219
4. Cramer's rule	221
5. Consistent and inconsistent systems	225
6. Homogeneous systems	231
7. Linear dependence of polynomials	235
8. Linear equations in a field	238

**14. ELIMINATION**

1. Definition of elimination	240
2. Resultants	241
3. Linear dependence and common factors	242
4. Condition for common roots	244
5. Two equations in two unknowns	251
6. Common factors of polynomials in two variables	253
7. Successive elimination	258

**APPENDIX**

I Mathematical induction	261
II Solutions of starred exercises	266

Numerical answers	277
-------------------	-----

Index	295
-------	-----

# ELEMENTARY THEORY OF EQUATIONS



## THE COMPLEX NUMBER SYSTEM

**1. Introduction** The complex number system did not suddenly appear like a butterfly from a cocoon, but developed gradually as the need for various types of numbers arose. In the theory of equations the need was that of solving algebraic equations.

If we suppose, as was once the case, that the only numbers known are the positive integers, then it is certainly not true that every equation has a root; for even a simple equation like  $x + 5 = 2$  cannot be solved if we restrict ourselves to positive integers. If we extend the number system by inventing the negative integers and zero, certain equations previously unsolvable become solvable; but some, like  $2x = 5$ , remain incapable of solution. If we extend the system further by creating the rational numbers, that is, the numbers expressible as ratios of integers, then every linear equation  $ax + b = 0$ , where  $a$  and  $b$  are rational and  $a$  is not zero, can be solved. But a quadratic equation like  $x^2 = 2$  is still unsolvable. Even when we create the irrational numbers, which constitute, together with the rationals, the system of real numbers, there are still some quadratic equations with no roots. Not until we construct the system of complex numbers do we obtain a domain in which all linear and quadratic equations are solvable. Fortunately, it then happens that every equation of degree higher than two is also solvable, so that from the point of view of the theory of equations no further extension of the number system is necessary.

How the number system is extended step by step from the positive integers to the complex numbers is an interesting logical story, which we cannot fully go into. We shall examine only the last step, forming the complex numbers from the real numbers.

**2. Complex numbers** In constructing the complex numbers from the reals we cannot begin by saying, "Let  $i = \sqrt{-1}$ ," since a

square root of  $-1$  does not exist until *after* the complex domain has been constructed. In terms of real numbers, what then are complex numbers? Essentially they are only pairs of real numbers,  $a$  and  $b$ , with which we operate in accordance with prescribed rules. Whether the pair is thought of in the form  $a + bi$  or some other form is immaterial. What is important is the respective roles of  $a$  and  $b$  in the complex number.

To distinguish between the roles of  $a$  and  $b$  we define a complex number as an *ordered* pair of real numbers and use the symbol  $(a, b)$  for it. We call  $a$  the first element and  $b$  the second element of the ordered pair.

Since the order of the numbers in an ordered pair is significant, the ordered pair  $(a, b)$  is different from the ordered  $\rightarrow (b, a)$  unless  $a$  and  $b$  are equal. That is,  $(a, b)$  and  $(c, d)$  are the same ordered pairs [indicated by  $(a, b) = (c, d)$ ] if and only if  $a = c$  and  $b = d$ .

We define two operations with complex numbers as follows:

- (1)  $(a, b) + (c, d) = (a + c, b + d).$
- (2)  $(a, b)(c, d) = (ac - bd, ad + bc).$

We call these addition and multiplication respectively. The results of the operations are called sums and products.

We can now prove that complex numbers obey laws for addition and multiplication similar to those for real numbers. Denoting complex numbers by capital letters,

- (3)  $A + B$  exists and is unique (Closure law for addition).
- (4)  $A + B = B + A$  (Commutative law for addition).
- (5)  $A + (B + C) = (A + B) + C$  (Associative law for addition).
- (6) There exists a unique complex number, denoted by  $0$ , such that  $A + 0 = A$  for every  $A$ . We call  $0$  the zero complex number or, briefly, zero. [We have  $0 = (0, 0)$ ]
- (7) For every  $A, B$  there exists one and only one  $C$  such that  $A = B + C$ . We write  $C = A - B$  and call  $C$  the difference between  $A$  and  $B$ . The operation of obtaining  $C$  is called subtraction. We define  $-A$  as  $0 - A$  and call it the negative of  $A$ .

The corresponding laws for multiplication are:

- (8)  $AB$  exists and is unique (Closure law for multiplication).
- (9)  $AB = BA$  (Commutative law for multiplication).



- (10)  $A(BC) = (AB)C$  (Associative law for multiplication).  
 (11) There exists a unique complex number, denoted by  $I$ , such that  $AI = A$  for every  $A$ . We call  $I$  the unity complex number or, briefly, unity. [We have  $I = (1, 0)$ .]  
 (12) For every  $A, B$ , provided  $B \neq 0$ , there exists one and only one  $C$  such that  $A = BC$ . We write  $C = A/B$  or  $C = A \div B$  and call  $C$  the quotient of  $A$  by  $B$ . The operation of obtaining  $C$  is called division. We call  $I \div B$  the reciprocal of  $B$ .

Two laws connecting addition and multiplication are:

- (13)  $A(B + C) = AB + AC$  (Distributive law).  
 (14)  $AB = 0$  if and only if  $A = 0$  or  $B = 0$  (Product law).

The proofs of the above laws are quite simple. We illustrate by proving (12).

Let  $A = (a, b)$ ,  $B = (c, d)$ ,  $C = (x, y)$ . Then, by (2),  $A = BC$  if and only if  $(a, b) = (cx - dy, cy + dx)$ . This is true if and only if

$$\begin{aligned} cx - dy &= a \\ dx + cy &= b \end{aligned}$$

By hypothesis  $B \neq 0$ . Hence either  $c$  or  $d$  is different from zero. Therefore  $c^2 + d^2$  is non-zero. Thus, solving the preceding equations for  $x$  and  $y$ ,

$$x = \frac{ac + bd}{c^2 + d^2}, \quad y = \frac{bc - ad}{c^2 + d^2}$$

This shows that there is one and only one  $C$ .

The laws (3)–(14) are not a complete list of all the rules ordinarily used in connection with addition, multiplication, subtraction, and division (called the rational operations), but the others can be derived from them. For instance, we show that if  $B \neq 0$  and  $C \neq 0$  then  $A/B = AC/BC$ .

If  $A/B = D$ , then

$$\begin{aligned} A &= BD \quad \text{by (12)} \\ AC &= (BD)C \quad \text{by (8)} \\ &= B(DC) \quad \text{by (10)} \\ &= B(CD) \quad \text{by (9)} \\ &= (BC)D \quad \text{by (10)} \\ \frac{AC}{BC} &= D \quad \text{by (12)} \end{aligned}$$

Without actually stating or proving all the common rules, we shall use them throughout the text.

### Exercises

- 1 Establish all the laws (3)–(14) above.
- 2 Prove:  $A - B = A + (-B)$ .
- 3 Prove:  $A(B - C) = AB - AC$ .
- 4 Prove:  $(-A)B = -AB$  and  $(-A)(-B) = AB$ .
- 5 Prove: If  $B \neq 0$ ,  $D \neq 0$  then  $(A/B) + (C/D) = (AD + BC)/BD$ .
- 6 Prove  $A0 = 0$  using only the laws (3)–(13), disregarding (1) and (2) and the fact that a complex number is an ordered pair of real numbers. [Hint: Start with  $A0 = A(0 + 0)$ .]
- 7 Using only (3)–(13) and the result of ex. 6, prove that  $AB = 0$  implies  $A = 0$  or  $B = 0$ .
- 8 In view of the definition (1) of  $(a, b) + (c, d)$ , it might seem natural to define  $(a, b)(c, d)$  as  $(ac, bd)$ . If this were done, which of the laws (3)–(14) would fail?
- 9 If we define  $(a, b)(c, d) = (ac, ad + bc)$  which of the laws (3)–(14) fail?

### 3. Real and imaginary complex numbers We note that

$$\begin{aligned}(a, 0) + (b, 0) &= (a + b, 0) \\(a, 0) - (b, 0) &= (a - b, 0) \\(a, 0)(b, 0) &= (ab, 0) \\(a, 0) \div (b, 0) &= (a \div b, 0) \quad \text{if } b \neq 0\end{aligned}$$

Thus, if we wish to perform rational operations with complex numbers of the form  $(x, 0)$ , we may disregard the zeros which appear as the second elements, perform the corresponding operations upon the first elements of the ordered pairs by treating them as real numbers, and then add a zero to the final result so as to make an ordered pair of the same form. Hence, as far as the rational operations are concerned, the complex numbers of the form  $(x, 0)$  have the same properties as the corresponding real numbers  $x$ .

This resemblance to the real numbers is increased if we define  $(a, 0)$  to be greater than  $(b, 0)$  if and only if  $a > b$ . Then not only with respect to the rational operations but also with respect to the relationship "greater than" do the complex numbers  $(x, 0)$  behave like the corresponding real numbers.

Because of this, a complex number of the form  $(x, 0)$  is called a real complex number. For convenience we shall denote it simply

by  $x$  even though for the moment there will be some ambiguity because  $x$  may denote either a real number or a real complex number.

We call  $(0, 1)$  the imaginary unit and denote it by  $i$ . We have  $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$ . Thus, in the complex domain the real complex number  $-1$  (not the real number  $-1$ ) has a square root.

We have  $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$ . Thus, every complex number is representable as the sum of a real complex number and a real complex number multiplied by  $i$ . Furthermore, this representation is possible in only one way. For if  $(a, b) = x + yi$ , where  $x$  and  $y$  are real complex numbers, then  $(a, b) = (x, 0) + (y, 0)(0, 1) = (x, y)$ , so that  $a = x$  and  $b = y$ .

Hereafter we shall always write  $a + bi$  instead of  $(a, b)$ . Furthermore, we shall never again deal with real numbers as such; instead we shall deal with the corresponding real complex numbers. There is no loss in doing this since the real complex numbers behave exactly like the real numbers. For brevity we shall hereafter refer to real complex numbers simply as real numbers.

To distinguish a complex number  $a + bi$  where  $b \neq 0$  from a real one (for which  $b = 0$ ), we call it imaginary. If  $a = 0$  and  $b \neq 0$  we call it a pure imaginary.

### Exercises

- 1 Express in  $a + bi$  form (Note:  $(a + bi)/(c + di)$  can be simplified quickly by multiplying numerator and denominator by  $c - di$ ):

a)  $(3 + 4i)^3$

e)  $\frac{3 - 4i}{2 - i}$

b)  $i^{27}$

f)  $\frac{1}{3 + 4i} + \frac{1}{3 - 4i}$

c)  $\frac{6}{1 - 2i}$

g)  $\frac{(1 + i)^4}{(1 - i)^2}$

d)  $i^{-9}$

- 2 Find all real numbers  $x$  and  $y$  so that

a)  $\frac{2}{1 - i} + x + yi = (x + yi)(1 + i)$

b)  $(x + i)^2 + (1/i) = (i - x)^2 + y + 1$

c)  $y^2 - (x - i)^2 + yi + 3 = (y + i)^2 - x^2 - 2x - 3i$

d)  $\frac{x - yi}{1 + i} + \frac{1}{i} = \frac{x}{2} + \frac{1}{1 - i}$

$$e) y^2 + (x - i)^2 + \frac{5y}{1 + 2i} = x^2 + (y + 2i)^2 + \frac{6}{1 + i}$$

$$f) (x - yi)(1 + i) + 2 - i = (1 + yi)(3 + i)$$

3 Express in the form stated, where  $a$  and  $b$  are real numbers:

a)  $5 - i$  in the form  $a(1 + i) + b(1 - i)$

b)  $1$  in the form  $a(2 + 3i) + b(1 + 2i)$

c)  $i$  in the form  $a + b(3 - 4i)$

d)  $i + 1$  in the form  $a(i + 6) + b(i - 6)$

e)  $2 - i$  in the form  $a(1 + 2i) + b(1 - 2i)$

4 Prove: If  $A$  and  $B$  are non-zero complex numbers whose ratio is not a real number, then for every complex number  $C$  there exists one and only one pair of real numbers  $x$  and  $y$  such that  $C = xA + yB$ . (The fact that every complex number is uniquely representable in the form  $x + yi$  is a special case with  $A = 1$  and  $B = i$ . Exercise 3 shows other special cases.)

5 We call  $a - bi$  the conjugate of  $a + bi$  and write  $a - bi = \overline{a + bi}$ . Prove:

a)  $\overline{A + B} = \overline{A} + \overline{B}$

d)  $\overline{\left(\frac{A}{B}\right)} = \frac{\overline{A}}{\overline{B}}$  if  $B \neq 0$

b)  $\overline{AB} = \overline{A}\overline{B}$

e) if  $A = \overline{B}$  then  $B = \overline{A}$

c)  $\overline{A - B} = \overline{A} - \overline{B}$

f)  $A\overline{B} + \overline{A}B$  is real

Extend (a) and (b) to  $\overline{A_1 + A_2 + \cdots + A_n}$  and  $\overline{A_1 A_2 \cdots A_n}$ .

6 Prove: If  $A^2 - 4B^2 + 1 = 0$ , then  $\overline{A}^2 - 4\overline{B}^2 + 1 = 0$ .

7 Prove: If  $C \neq 0$ ,  $D \neq 0$ , then  $A/B = C/D$  if and only if  $\overline{A}/\overline{B} = \overline{C}/\overline{D}$ .

8 Prove: A complex number is real if and only if it is its own conjugate.

9 Prove: A non-zero complex number is a pure imaginary if and only if it is the negative of its conjugate.

10 Imaginary complex numbers  $A$  and  $B$  are conjugates of each other if and only if their sum is real and their difference is a pure imaginary.

11 If  $A$  is an imaginary complex number then  $B$  is the conjugate of  $A$  if and only if  $A + B$  and  $AB$  are real.

12 Is  $-2i$  real, imaginary, positive, negative, odd, even, rational, irrational?

13 Find two complex numbers whose squares are

a)  $i$

c)  $5 + 12i$

b)  $3 - 4i$

d)  $24 - 7i$

14 Prove: A non-zero complex number has two square roots.

15 If  $\omega = \frac{1}{2}(-1 \pm i\sqrt{3})$  show that  $\omega^2 = \frac{1}{2}(-1 \mp i\sqrt{3})$  and that  $1, \omega, \omega^2$  are all the cube roots of 1.

**4. Modulus** We recall that ordered pairs of real numbers are used in the familiar method of setting up a rectangular coordinate system in a plane. Each point in the plane is represented by an ordered pair of real numbers  $(x, y)$  called the coordinates of the point.

Since complex numbers have been defined as ordered pairs of real numbers, this suggests that we may represent complex numbers by points in a plane. We do this in the obvious way of associating with every complex number  $a + bi$ , where  $a$  and  $b$  are real, the point whose coordinates are  $(a, b)$ . In this manner every complex number is represented by a unique point and, conversely, every point in the plane represents a unique complex number. We have what is referred to as a one-to-one correspondence between the complex numbers and the points in the plane.

In this correspondence, the real numbers are represented by the points on the  $x$  axis and every point on the  $x$  axis represents a real number. The  $x$  axis, therefore, is called the real axis.

Pure imaginary numbers correspond to points on the  $y$  axis which, therefore, is called the imaginary axis.

If  $a + bi$  is a complex number, with  $a$  and  $b$  real, the real non-negative square root of  $a^2 + b^2$  is called the modulus of  $a + bi$  and is denoted by  $|a + bi|$ . With the usual agreement that when  $x \geq 0$  the symbol  $\sqrt{x}$  denotes the non-negative square root of  $x$ , we may write  $|a + bi| = \sqrt{a^2 + b^2}$ .

Geometrically,  $|a + bi|$  is the distance from the origin to the point  $(a, b)$  which represents  $a + bi$ .

The following theorems will be used frequently.

#### THEOREM

$$|AB| = |A||B|.$$

*Proof:* Let  $A = a + bi$ ,  $B = c + di$ . Then

$$\begin{aligned} |AB| &= |(ac - bd) + (ad + bc)i| = \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} \\ &= \sqrt{(a^2 + b^2)(c^2 + d^2)} = \sqrt{a^2 + b^2} \sqrt{c^2 + d^2} = |A||B| \end{aligned}$$

#### COROLLARY

$$|A_1 A_2 \cdots A_n| = |A_1| |A_2| \cdots |A_n|$$

This follows from the theorem by mathematical induction. (See Appendix I for a discussion of mathematical induction.)

### THEOREM

If  $B \neq 0$  then 
$$\left| \frac{A}{B} \right| = \frac{|A|}{|B|}.$$

*Proof:* Let  $C = A/B$ . Then  $A = BC$ . By the preceding theorem  $|A| = |B||C|$ . Hence  $|C| = |A|/|B|$ .

### THEOREM

$|A + B| \leq |A| + |B|$ .

*Proof:* Let  $A = a + bi$ ,  $B = c + di$ . Then

$$\begin{aligned} |A + B| &= |(a + c) + (b + d)i| = \sqrt{(a + c)^2 + (b + d)^2} \\ |A| + |B| &= \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \end{aligned}$$

If  $|A + B| \leq |A| + |B|$ , then  $\sqrt{(a + c)^2 + (b + d)^2} \leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}$ . Squaring both sides, canceling common terms, and dividing by 2, we obtain

$$ac + bd \leq \sqrt{a^2 + b^2} \sqrt{c^2 + d^2}$$

Conversely, since all the steps are reversible, if we establish the last inequality we shall have proved  $|A + B| \leq |A| + |B|$ .

If  $ac + bd$  is negative or zero, the inequality is obvious, since the right side cannot be negative.

If  $ac + bd$  is positive, then, squaring both sides and canceling common terms, the inequality holds if and only if

$$2abcd \leq a^2d^2 + b^2c^2,$$

or, by transposing, if and only if  $0 \leq (ad - bc)^2$ .

Since this last inequality is obviously true, the desired result is established.

### COROLLARY

$|A_1 + A_2 + \cdots + A_n| \leq |A_1| + |A_2| + \cdots + |A_n|$ .

This follows from the theorem by mathematical induction.

## THEOREM

$$|A + B| \geq |A| - |B|.$$

*Proof:* Let  $C = A - B$ . Then  $A = B + C$ . By the preceding theorem  $|A| = |B + C| \leq |B| + |C|$ . Therefore  $|C| \geq |A| - |B|$ .

## Exercises

- 1 Prove: A complex number is zero if and only if its modulus is zero.
- 2 Prove: (a)  $|-A| = |A|$  (b)  $|\bar{A}| = |A|$ .
- 3 Prove:  $||A| - |B|| \leq |A - B| \leq |A| + |B|$ .
- 4 Prove:  $|A + B| = |A| + |B|$  if and only if there exists a real non-negative number  $\lambda$  such that  $A = \lambda B$  or  $B = \lambda A$ .
- 5 Prove: If  $x$  is real then  $|x| = x$  if  $x \geq 0$  and  $|x| = -x$  if  $x < 0$ . (Thus, the modulus of a real number is the same as its absolute value.)
- 6 Interpret geometrically the theorem that  $|A + B| \leq |A| + |B|$ .
- 7 Prove: If  $A, B$  are represented by the points  $P_1, P_2$  respectively, then  $|A - B|$  is the distance between  $P_1$  and  $P_2$ .
- 8 Prove: If the complex numbers  $A, B, C$  are represented by the points  $P, Q, R$  respectively, and if  $P$  and  $Q$  are not on a line with the origin  $O$ , then  $A + B = C$  if and only if  $OPRQ$  is a parallelogram.
- 9 Locate geometrically the points for which the corresponding complex numbers  $z$  satisfy:
  - a)  $|z| = 1$
  - b)  $|z - 2| \leq 1$
  - c)  $|z - 2| = |z - 1$
  - d)  $|z + 1| = |z| + 1$
  - e)  $|z - 1|^2 + |z + 1|^2 = (|z - 1| + |z + 1|)^2$
- 10 Prove: If  $A \neq 0$  then  $A$  and  $B$  are conjugates if and only if  $AB = |A|^2$ .
- 11 If  $z = x + yi$ , where  $x$  and  $y$  are real prove  $|z| \geq (|x| + |y|)/\sqrt{2}$ .
- 12 Prove:  $|A| = |A + 1| = 1$  if and only if  $A^2 + A + 1 = 0$ .
- 13 Find the modulus of each of the following from the moduli of the factors:

$$a) \frac{(1 - \sqrt{3}i)^3}{i(-2 + 2i)^4}$$

$$d) \frac{(1 + i)(\sqrt{3} + i)^3}{(1 - \sqrt{3}i)^3}$$

$$b) \left[ \frac{-3i(2 - 2i)(-\sqrt{3} - i)^4}{3 - 3i} \right]^4$$

$$e) \frac{(i - 1)^6(\sqrt{3} - i)^4}{(2 + 2i)^4}$$

$$c) \frac{(1 - i)^6}{(2 + 2i)^4(i - \sqrt{3})^3}$$

$$f) \left( \frac{1 + i}{\sqrt{2}} \right)^{100} \left( \frac{1 + i\sqrt{3}}{2} \right)^{80}$$

**5.\* Polar form** If  $a + bi \neq 0$  we define an angle  $\theta$  to be an amplitude of  $a + bi$  if  $\cos \theta = \frac{a}{|a + bi|}$  and  $\sin \theta = \frac{b}{|a + bi|}$ . Geometrically, an amplitude is any angle (measured clockwise or counterclockwise) whose initial side is the positive part of the  $x$  axis and whose terminal side is the ray which emanates from the origin and which passes through the point  $(a, b)$ .

If  $\theta$  is an amplitude of  $a + bi$ , then  $a = |a + bi| \cos \theta$  and  $b = |a + bi| \sin \theta$ . Hence  $a + bi = |a + bi| (\cos \theta + i \sin \theta) = \sqrt{a^2 + b^2} (\cos \theta + i \sin \theta)$ . This expression is called a polar or trigonometric form for  $a + bi$ .

*Example* Express  $1 - i$  in polar form.

Here  $a = 1$ ,  $b = -1$ ,  $|a + bi| = \sqrt{a^2 + b^2} = \sqrt{2}$ ,  $\cos \theta = \frac{1}{\sqrt{2}}$ ,  $\sin \theta = -\frac{1}{\sqrt{2}}$ . Thus  $315^\circ$  is an amplitude of  $1 - i$ . Hence  $1 - i = \sqrt{2} (\cos 315^\circ + i \sin 315^\circ)$ .

### THEOREM

If  $\theta$  is an amplitude of  $A$  and  $\varphi$  an amplitude of  $B$ , then  $\theta + \varphi$  is an amplitude of  $AB$ .

*Proof:*

$$\begin{aligned} A &= |A| (\cos \theta + i \sin \theta), \quad B = |B| (\cos \varphi + i \sin \varphi) \\ AB &= |A||B| [\cos \theta \cos \varphi - \sin \theta \sin \varphi + i(\sin \theta \cos \varphi \\ &\quad + \cos \theta \sin \varphi)] \\ &= |A||B| [\cos (\theta + \varphi) + i \sin (\theta + \varphi)] \\ &= a + bi \end{aligned}$$

where  $a = |A||B| \cos (\theta + \varphi)$  and  $b = |A||B| \sin (\theta + \varphi)$ .

An angle  $\alpha$  is an amplitude of  $AB$  if and only if

$$\begin{aligned} \cos \alpha &= \frac{a}{|AB|} = \frac{|A||B| \cos (\theta + \varphi)}{|AB|} = \cos (\theta + \varphi) \\ \sin \alpha &= \frac{b}{|AB|} = \frac{|A||B| \sin (\theta + \varphi)}{|AB|} = \sin (\theta + \varphi) \end{aligned}$$

Obviously,  $\alpha = \theta + \varphi$  satisfies these conditions.

### COROLLARY

(*de Moivre's theorem*) If  $n$  is a positive integer and  $\theta$  an amplitude of  $a + bi$ , then  $(a + bi)^n = |a + bi|^n (\cos n\theta + i \sin n\theta)$ .

\* §5 and §6 are not used elsewhere in the text.



**Proof:** This follows from the theorem and the first corollary in §4 (using mathematical induction on  $n$ ) by considering  $A_1 A_2 \cdots A_n$ , where each of the  $A$ 's is  $a + bi$ .

**Example** Express  $(1 - i)^{12}$  in  $a + bi$  form.

We have

$$\begin{aligned} 1 - i &= \sqrt{2} (\cos 315^\circ + i \sin 315^\circ) \\ (1 - i)^{12} &= (\sqrt{2})^{12} (\cos 12 \cdot 315^\circ + i \sin 12 \cdot 315^\circ) \\ &= 2^6 (\cos 180^\circ + i \sin 180^\circ) \\ &= 64(-1 + 0i) = -64 \end{aligned}$$

### Exercises

- 1 Prove: A complex number has an amplitude of  $0^\circ$  if and only if the number is real and positive.
- 2 Prove. If  $\theta$  is an amplitude of  $A$  and  $\varphi$  an amplitude of  $B$ , then  $\theta - \varphi$  is an amplitude of  $1/B$ .
- 3 By finding the modulus and an amplitude of the result from the moduli and amplitudes of the factors, simplify.

$$a) \frac{(1 - i\sqrt{3})^3}{i(-2 + 2i)^4}$$

$$d) \frac{(1 + i)(\sqrt{3} + i)^3}{(1 - \sqrt{3}i)^3}$$

$$b) \left[ \frac{-3i(2 + 2i)(-\sqrt{3} - i)}{3 - 3i} \right]^4$$

$$e) \frac{(i - 1)^6(\sqrt{3} - i)^4}{(2 + 2i)^4}$$

$$c) \frac{(1 - i)^6}{(2 + 2i)^4(i - \sqrt{3})^4}$$

$$f) \left( \frac{1 + i}{\sqrt{2}} \right)^{100} \left( \frac{1 + i\sqrt{3}}{2} \right)^{30}$$

- 4 Express  $\cos \theta - i \sin \theta$  in polar form. Show that  $(\cos \theta - i \sin \theta)^n = \cos n\theta - i \sin n\theta$ , where  $n$  is a positive integer.
- 5 Prove. If  $n$  is a positive integer,  $(\cos \theta + i \sin \theta)^n = \cos(-n\theta) + i \sin(-n\theta)$ .
- 6 Using de Moivre's theorem and the binomial theorem, express  $\cos 5\theta$  and  $\sin 5\theta$  in terms of  $\sin \theta$  and  $\cos \theta$ .
- 7 Prove. If  $A \neq 0$ ,  $B \neq 0$ , then  $|A + B| = |A| + |B|$  if and only if  $A$  and  $B$  have a common amplitude.
- 8 Prove: If  $\theta$  is an amplitude of  $A$ , then all the amplitudes of  $A$  are given by  $\theta + n360^\circ$  where  $n$  is any integer.
- 9 Prove: If  $A = r(\cos \varphi + i \sin \varphi)$  where  $r$  is positive, then  $r(\cos \varphi + i \sin \varphi)$  is a polar form for  $A$ .
- 10 Prove. If  $\theta$  is an amplitude of  $A$  and  $A = r(\cos \theta + i \sin \theta)$  where  $r$  is a complex number, then  $r(\cos \theta + i \sin \theta)$  is a polar form for  $A$ .

**6. Roots of complex numbers** If  $n$  is a positive integer and  $B^n = A$ ,  $B$  is called an  $n$ th root of  $A$ .

If  $A$  is real and positive, it is shown in the theory of real numbers that there exists a unique positive  $n$ th root of  $A$ . It is usual to denote this root by  $\sqrt[n]{A}$ .

It is natural to inquire whether, for a given  $n$ , a complex number has  $n$ th roots and, if so, how many. For the number 0 there is obviously a unique  $n$ th root. For other numbers these questions are answered by:

### THEOREM

*If  $n$  is a positive integer and  $A \neq 0$ , there are exactly  $n$   $n$ th roots of  $A$ .*

*Proof:* We consider first the special case when  $A = 1$ .

If  $B$  is an  $n$ th root of 1, then  $|B^n| = |1| = 1$ . Hence (§4),  $|B|^n = 1$ . Therefore  $|B| = 1$ . Thus, the  $n$ th roots of 1 are to be found among the numbers expressible in polar form as  $\cos \theta + i \sin \theta$ .

We can always choose the amplitude  $\theta$  so that  $0^\circ \leq \theta < 360^\circ$ . Suppose this done.

By de Moivre's theorem  $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$ . Therefore,  $\cos \theta + i \sin \theta$  is an  $n$ th root of 1 if and only if  $\cos n\theta = 1$  and  $\sin n\theta = 0$ . This will be true if and only if  $n\theta$  is an integral multiple of  $360^\circ$ .

Since  $0^\circ \leq \theta < 360^\circ$ ,  $0 \leq n\theta < n \cdot 360^\circ$ . Therefore,  $\cos \theta + i \sin \theta$  is an  $n$ th root of 1 if and only if  $n\theta$  is one of the angles  $0^\circ, 360^\circ, 2 \cdot 360^\circ, \dots, (n-1)360^\circ$ ; hence, if and only if  $\theta$  is one of the angles  $0^\circ, \frac{360^\circ}{n}, \frac{2 \cdot 360^\circ}{n}, \dots, \frac{(n-1)360^\circ}{n}$ .

Letting  $\omega_k = \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n}$  for  $k = 0, 1, 2, \dots, n-1$ , it follows that  $\omega_0, \omega_1, \dots, \omega_{n-1}$  are  $n$ th roots of 1 and that there are no others. To complete the proof for  $A = 1$  we have only to show that no two of  $\omega_0, \omega_1, \dots, \omega_{n-1}$  are equal.

Suppose, contrariwise, that  $\omega_p = \omega_q$  where, to be specific,  $p > q$ . Then  $\cos \frac{p \cdot 360^\circ}{n} = \cos \frac{q \cdot 360^\circ}{n}$ ,  $\sin \frac{p \cdot 360^\circ}{n} = \sin \frac{q \cdot 360^\circ}{n}$ ,

$$\begin{aligned}
 \cos \frac{(p-q)360^\circ}{n} &= \cos \left( \frac{p \cdot 360^\circ}{n} - \frac{q \cdot 360^\circ}{n} \right) \\
 &= \cos \frac{p \cdot 360^\circ}{n} \cos \frac{q \cdot 360^\circ}{n} + \sin \frac{p \cdot 360^\circ}{n} \sin \frac{q \cdot 360^\circ}{n} \\
 &= \cos^2 \frac{p \cdot 360^\circ}{n} + \sin^2 \frac{p \cdot 360^\circ}{n} = 1 \\
 &\quad (\text{since } \cos^2 \varphi + \sin^2 \varphi = 1 \text{ for all angles})
 \end{aligned}$$

Thus,  $\frac{(p-q)360^\circ}{n}$  is an integral multiple of  $360^\circ$ , that is,  $\frac{p-q}{n}$  is an integer. But,  $0 \leq q < p < n$ ; hence,  $0 < p-q < n$  and  $0 < \frac{p-q}{n} < 1$ , so that  $\frac{p-q}{n}$  cannot be an integer.

Now, returning to the general case, let  $A = |A| (\cos \varphi + i \sin \varphi)$ . Then  $\alpha = \sqrt[n]{|A|} \left( \cos \frac{\varphi}{n} + i \sin \frac{\varphi}{n} \right)$  is one  $n$ th root of  $A$ . For, by de Moivre's theorem,  $\alpha^n = |A| (\cos \varphi + i \sin \varphi) = A$ .

If  $B$  is any  $n$ th root of  $A$ , then  $(B/\alpha)^n = B^n/\alpha^n = A/A = 1$ , so that  $B/\alpha$  is an  $n$ th root of 1. Conversely, if  $B$  is a complex number such that  $B/\alpha$  is an  $n$ th root of 1, then  $B^n/\alpha^n = (B/\alpha)^n = 1$ , so that  $B^n = \alpha^n = A$ . Thus,  $B$  is an  $n$ th root of  $A$  if and only if  $B/\alpha$  is one of the numbers  $\omega_0, \omega_1, \dots, \omega_{n-1}$ ; hence, if and only if  $B$  is one of the numbers  $\alpha\omega_0, \alpha\omega_1, \dots, \alpha\omega_{n-1}$ . Since  $\omega_0, \omega_1, \dots, \omega_{n-1}$  are distinct, these  $n$  numbers are distinct, and the theorem is proved.

#### COROLLARY

If  $\varphi$  is an amplitude of  $A$ , the  $n$ th roots of  $A$  are  $\sqrt[n]{|A|} [\cos (\varphi + k360^\circ)/(n) + i \sin (\varphi + k360^\circ)/(n)]$   $k = 0, 1, \dots, n-1$ .

*Proof:* The  $n$ th roots of  $A$  are

$$\begin{aligned}
 \alpha\omega_k &= \sqrt[n]{|A|} \left( \cos \frac{\varphi}{n} + i \sin \frac{\varphi}{n} \right) \left( \cos \frac{k \cdot 360^\circ}{n} + i \sin \frac{k \cdot 360^\circ}{n} \right) \\
 &\quad (k = 0, 1, \dots, n-1) \\
 &= \sqrt[n]{|A|} \left( \cos \frac{\varphi + k360^\circ}{n} + i \sin \frac{\varphi + k360^\circ}{n} \right)
 \end{aligned}$$

**Example** Find the fourth roots of  $-1 + i\sqrt{3}$ .

In polar form,  $-1 + i\sqrt{3} = 2(\cos 120^\circ + i \sin 120^\circ)$ . Hence, the fourth roots are  $\sqrt[4]{2} (\cos (120^\circ + k360^\circ)/(4) + i \sin (120^\circ +$

$k360^\circ)/(4))$  for  $k = 0, 1, 2, 3$ . For these values of  $k$  we obtain

$$\begin{aligned}\sqrt[4]{2} (\cos 30^\circ + i \sin 30^\circ) &= \sqrt[4]{2} (\tfrac{1}{2} \sqrt{3} + \tfrac{1}{2}i) \\ \sqrt[4]{2} (\cos 120^\circ + i \sin 120^\circ) &= \sqrt[4]{2} (-\tfrac{1}{2} + \tfrac{1}{2}i \sqrt{3}) \\ \sqrt[4]{2} (\cos 210^\circ + i \sin 210^\circ) &= \sqrt[4]{2} (-\tfrac{1}{2} \sqrt{3} - \tfrac{1}{2}i) \\ \sqrt[4]{2} (\cos 300^\circ + i \sin 300^\circ) &= \sqrt[4]{2} (\tfrac{1}{2} - \tfrac{1}{2}i \sqrt{3})\end{aligned}$$

### Exercises

#### 1 Find the

- |                          |                                     |
|--------------------------|-------------------------------------|
| a) cube roots of $-27$   | d) cube roots of $27i$              |
| b) sixth roots of $64$   | e) square roots of $2 + 2i\sqrt{3}$ |
| c) fourth roots of $-16$ | f) eighth roots of $1$              |

- If  $\omega = \cos (360^\circ/n) + i \sin (360^\circ/n)$ , show that  $\omega^0 = 1, \omega, \omega^2, \dots, \omega^{n-1}$  are the  $n$ th roots of  $1$ . Hence show also that if  $B$  is an  $n$ th root of  $A \neq 0$ , then  $B, \omega B, \dots, \omega^{n-1}B$  are the  $n$ th roots of  $A$ .
- Prove: The reciprocals of the  $n$ th roots of  $1$  are the  $n$ th roots of  $1$ .
- Prove: If  $n$  is odd, the squares of the  $n$ th roots of  $1$  are the  $n$ th roots of  $1$ .
- Prove: If  $\theta$  is an amplitude of  $A$  and  $\epsilon = \cos (\theta/n) + i \sin (\theta/n)$  and  $\alpha_1, \alpha_2, \dots, \alpha_n$  are the  $n$ th roots of  $|A|$ , then  $\epsilon\alpha_1, \epsilon\alpha_2, \dots, \epsilon\alpha_n$  are the  $n$ th roots of  $A$ .
- Prove: The conjugates of the  $n$ th roots of  $A$  are the  $n$ th roots of the conjugate of  $A$ .
- Prove: If  $A \neq 0$  has exactly one real  $n$ th root, then  $A$  is real,  $n$  is odd, and the real  $n$ th root has the same sign as  $A$ .
- Prove: If  $A$  has more than one real  $n$ th root, then  $A$  is real and positive,  $n$  is even, there are exactly two real  $n$ th roots, and they are the negatives of each other.
- If  $\theta$  is an amplitude of  $A$  and  $p+1, p+2, \dots, p+n$  are any  $n$  consecutive integers, the  $n$ th roots of  $A$  are  $\sqrt[n]{|A|} [\cos (\theta + k360^\circ/n) + i \sin (\theta + k360^\circ/n)]$  ( $k = p+1, p+2, \dots, p+n$ ).
- Prove: If  $A$  and  $A+1$  are  $n$ th roots of  $1$ , then  $n$  is divisible by  $6$  and  $A$  is an imaginary cube root of  $1$ .

## POLYNOMIALS IN ONE VARIABLE

**1. Definition of polynomial** If  $x$  and  $y$  are variables and to each value of  $x$  there corresponds in some prescribed manner a definite value of  $y$ , then  $y$  is said to be a (one-valued) function of  $x$ . For example:

- (a) If  $x$  denotes any real number, then  $y = x^2$  is a function of  $x$ .
- (b) If  $x$  is any positive integer and  $y$  the number of positive prime integers less than  $x$ , then  $y$  is a function of  $x$ ; in this case there is no simple way to express  $y$  in terms of  $x$ .

We use a symbol like  $f(x)$  and  $g(x)$ , to denote a function of  $x$ . We use the same symbol to stand for the number which corresponds to a given value of  $x$ . Thus, in example (a),  $f(x) = x^2$ ,  $f(1) = 1^2 = 1$ ,  $f(2) = 2^2 = 4$ , etc.

When there is no danger of misunderstanding we shall often write  $f$ ,  $g$ , etc., in place of the complete symbols  $f(x)$ ,  $g(x)$ , etc.

If  $f(x)$  is a function of  $x$ , where  $x$  may be any complex number, and if there exists an integer  $n \geq 0$  and complex numbers  $a_0, a_1, \dots, a_n$  such that

$$(1) \quad f(x) \equiv a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

(where the identity sign  $\equiv$  indicates that the equality holds for all values of  $x$ ), then  $f(x)$  is said to be a polynomial in  $x$  or, briefly, a polynomial.

The numbers  $a_0, a_1, \dots, a_n$  are called the coefficients.  $a_n$  is called the coefficient of  $x^{n-i}$ .  $a_n$  is called the constant term and  $a_0$  the leading coefficient.

Examples of polynomials are.

- (a)  $(1+i)x^3 - \sqrt{2}x + 1$ , with  $n = 3$ ,  $a_0 = 1+i$ ,  $a_1 = 0$ ,  $a_2 = -\sqrt{2}$ ,  $a_3 = 1$
- (b)  $7$ , with  $n = 0$ ,  $a_0 = 7$
- (c)  $0$ , with  $n = 0$ ,  $a_0 = 0$ .

If  $a_0 \neq 0$  in (1),  $f(x)$  is said to be of degree  $n$ . Thus (a) is of degree 3 and (b) is of degree 0.

A polynomial which has the same value for every value of  $x$  is called a constant polynomial or, briefly, a constant. If  $f(x) \equiv 0$  it is called the zero polynomial.

A polynomial of degree 1 is called linear; of degree 2, quadratic; of degree 3, cubic; of degree 4, quartic or biquadratic; of degree 5, quintic; etc.

It is conceivable, until we have proved otherwise, that two different expressions of the form (1) may have equal values for all values of  $x$  and, therefore, represent the same polynomial. Thus, for the present, we have no right to speak of the degree of a polynomial but only of a degree.

Throughout the remainder of the text all symbols for functions denote polynomials unless otherwise stated.

## 2. Sums and products of polynomials If

$$\begin{aligned} f &= a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ g &= b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m \end{aligned}$$

it is evident that  $f + g$ ,  $f - g$ , and  $fg$  are also polynomials.

In particular,  $fg \equiv a_0b_0x^{m+n} + (a_0b_1 + a_1b_0)x^{m+n-1} + \cdots + a_nb_m$ . Thus, if  $f$  is of degree  $n$ , i.e.,  $a_0 \neq 0$  and  $g$  of degree  $m$ , i.e.,  $b_0 \neq 0$ , then  $fg$  is of degree  $m + n$ .

If  $a_0 \neq 0$ ,  $b_0 \neq 0$ , and  $m$  and  $n$  are unequal,  $f + g$  has a degree equal to the larger of  $m$  and  $n$ . But if  $m = n$ ,  $f + g$  may be the zero polynomial, since corresponding terms in  $f$  and  $g$  may cancel each other; otherwise it will have a degree not exceeding  $n$ .

These remarks about two polynomials extend to any number of polynomials. If  $f_1, f_2, \dots, f_p$  are of degrees  $n_1, n_2, \dots, n_p$  respectively, then

- (a)  $f_1f_2 \cdots f_p$  is of degree  $n_1 + n_2 + \cdots + n_p$
- (b) If  $f_1 + f_2 + \cdots + f_p$  is not the zero polynomial it has a degree not exceeding the largest of  $n_1, n_2, \dots, n_p$ . If one of  $n_1, n_2, \dots, n_p$  exceeds all the others,  $f_1 + f_2 + \cdots + f_p$  has a degree equal to that one.

**3. Factor theorem** A value of  $x$  for which the corresponding value of  $f(x)$  is zero is called a root or zero of  $f$ . For such a value of

$x$  the polynomial is said to vanish. A root of  $f$  is also called a root of the equation  $f(x) = 0$ .

If  $f(x) \equiv (x - r)g(x)$ , where  $r$  is a complex number, then  $f(r) = (r - r)g(r) = 0$ , i.e.,  $r$  is a root of  $f$ . We now establish the converse, called the factor theorem.

**Lemma\*** If  $n \geq 1$  and  $r$  is a complex number, then  $x^n - r^n \equiv (x - r)g(x)$  where  $g(x)$  is of degree  $n - 1$ .

*Proof:* If  $g(x) \equiv x^{n-1} + rx^{n-2} + \dots + r^{n-2}x + r^{n-1}$ , direct multiplication shows that  $(x - r)g(x) \equiv x^n - r^n$ .

#### THEOREM :-

If  $r$  is a root of  $f(x)$  then  $f(x) \equiv (x - r)g(x)$ , and if  $f$  is of degree  $n$  then  $g$  is of degree  $n - 1$ .

*Proof:* If  $f$  is the zero polynomial, we may take  $g$  as the zero polynomial.

If  $f$  is not the zero polynomial, it is expressible in the form (1) of §1 with at least one non-zero coefficient. Hence we may and do suppose that  $a_0 \neq 0$ .

If  $n = 0$  then  $f(x) \equiv a_0$ . Hence  $f(r) = a_0 \neq 0$ . Thus, this situation is impossible.

For  $n > 0$ ,  $f(x) \equiv f(x) - f(r) \equiv a_0(x^n - r^n) + a_1(x^{n-1} - r^{n-1}) + \dots + a_{n-1}(x - r)$ . By the lemma,  $f(x) \equiv a_0(x - r)g_0(x) + a_1(x - r)g_1(x) + \dots + a_{n-1}(x - r)g_{n-1}(x)$  where  $g_0(x)$ ,  $g_1(x)$ ,  $\dots$ ,  $g_{n-1}(x)$  are of degree  $n - 1$ ,  $n - 2$ ,  $\dots$ ,  $0$  respectively. Hence  $f(x) \equiv (x - r)[a_0g_0(x) + a_1g_1(x) + \dots + a_{n-1}g_{n-1}(x)] \equiv (x - r)g(x)$ .

Since  $a_0 \neq 0$ ,  $a_0g_0(x)$  is of degree  $n - 1$ . Since each of  $a_1g_1(x)$ ,  $\dots$ ,  $a_{n-1}g_{n-1}(x)$  is either the zero polynomial or of degree less than  $n - 1$ ,  $g(x)$  is of degree  $n - 1$  (§2), and the theorem is proved.

**Remark** The factor theorem gives no information concerning the existence of roots of a polynomial. It merely states that a polynomial may be expressed in a certain way if it has a root.

**4. Uniqueness of representation** Not every polynomial has a root. Thus, if  $f(x) - a_0 \neq 0$ , there is no value of  $x$  for which  $f(x) = 0$ . A linear polynomial  $a_0x + a_1$ ,  $a_0 \neq 0$ , has exactly one

\* A lemma is a preliminary theorem.

root. A quadratic polynomial  $a_0x^2 + a_1x + a_2$ ,  $a_0 \neq 0$ , has two roots,  $(-a_1 \pm \sqrt{a_1^2 - 4a_0a_2})/2a_0$ , if  $a_1^2 - 4a_0a_2 \neq 0$ ; but if  $a_1^2 - 4a_0a_2 = 0$  then there is only one root. These observations illustrate the following theorem.

### THEOREM

*A polynomial of degree  $n$  cannot have more than  $n$  roots.*

*Proof:* We have already seen that this is true for  $n = 0$  and  $n = 1$ . Proceeding by mathematical induction, we assume that a polynomial of degree  $k$  has at most  $k$  roots.

Let  $f(x) \equiv a_0x^{k+1} + a_1x^k + \cdots + a_kx + a_{k+1}$ ,  $a_0 \neq 0$ . Suppose it has at least  $k + 2$  roots  $r_1, r_2, \dots, r_{k+2}$ .

By the factor theorem,  $f(x) \equiv (x - r_{k+2})g(x)$  where  $g(x)$  is of degree  $k$ . Letting  $x = r_i$ , where  $i$  is any one of the integers  $1, 2, \dots, k + 1$ ,  $0 = f(r_i) = (r_i - r_{k+2})g(r_i)$ . Since  $r_i \neq r_{k+2}$ , therefore  $g(r_i) = 0$ .

Thus,  $g(x)$  is a polynomial of degree  $k$  with  $k + 1$  roots  $r_1, r_2, \dots, r_{k+1}$ . This contradicts the hypothesis of the induction. Therefore  $f$  cannot have more than  $k + 1$  roots.

By the principle of mathematical induction, the theorem is proved.

### THEOREM

*If  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$  vanishes for infinitely many values of  $x$ , then  $a_0 = a_1 = \cdots = a_{n-1} = a_n = 0$ .*

*Proof:* If not all the coefficients are zero, let  $a_k$  be the coefficient with smallest subscript which is different from zero. Then the given polynomial is of degree  $n - k$  and, therefore, cannot vanish for more than  $n - k$  values of  $x$ . This contradicts the hypothesis. Hence, all the coefficients must be zero, and the theorem is proved.

### COROLLARY

*If  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0$ , then  $a_0 = a_1 = \cdots = a_{n-1} = a_n = 0$ .*

*Proof:* Since the polynomial vanishes for every value of  $x$ , the theorem applies and gives the desired result.

*Remark* The corollary shows that there is no way of expressing the zero polynomial in the form (1) of §1 with a non-zero coefficient. Therefore, the zero polynomial has no degree.



## THEOREM

If  $f(x)$  is a polynomial other than the zero polynomial, there is an expression  $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  with  $a_0 \neq 0$  such that  $f \equiv a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ . If also  $f \equiv b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m$ , then  $m \geq n$  and  $b_0 = b_1 = \dots = b_{m-n-1} = 0$ ,  $b_{m-n} = a_0$ ,  $b_{m-n+1} = a_1$ ,  $\dots$ ,  $b_m = a_n$ .

*Proof:* By definition,  $f$  can be expressed in the form (1) of §1. Since  $f$  is not the zero polynomial, at least one of the coefficients is different from zero. If  $a_k$  is the coefficient with smallest subscript which is non zero, then  $f = a_kx^{n-k} + \dots + a_n$ ,  $a_k \neq 0$ , which proves the first part of the theorem.

To prove the second part, suppose

$$a_0x^n + \dots + a_n \equiv b_0x^m + \dots + b_m, a_0 \neq 0$$

As before, not every  $b$  can be zero. Let  $b_l$  be the  $b$  with smallest subscript which is non-zero. Then, by subtraction,  $(a_0x^n + \dots + a_n) - (b_lx^{m-l} + \dots + b_m) \equiv 0$ .

If  $n > m - l$ , the left side is of degree  $n$  whereas the right side is the zero polynomial which has no degree. This is impossible.

Similarly  $n < m - l$  is impossible.

Therefore,  $n = m - l$ , so that  $l = m - n$ . Hence  $m - n \geq 0$  and  $b_0 = b_1 = \dots = b_{m-n-1} = 0$ . Also

$$(a_0x^n + \dots + a_n) - (b_{m-n}x^n + b_{m-n+1}x^{n-1} + \dots + b_m) \equiv 0$$

$$(a_0 - b_{m-n})x^n + (a_1 - b_{m-n+1})x^{n-1} + \dots + (a_n - b_m) \equiv 0$$

By the preceding corollary, all the coefficients in the last expression are zero, so that the theorem is proved.

*Remark* This theorem and the preceding corollary show that a polynomial can be expressed in the form (1) of §1 in essentially only one way. It follows that the degree of a polynomial is unique.

*Example 1* If  $fg = fh$  and  $f \neq 0$ , then  $g = h$ . (Cancellation law for polynomials)

(From the given equality it follows, by division by  $f$ , that  $g = h$  for every value of  $x$  for which  $f \neq 0$ . But there may be values of  $x$  for which  $f$  does vanish, so that we cannot immediately conclude that  $g \equiv h$ )

*Proof:* By subtraction,  $f(g - h) \equiv 0$ . Since  $f \neq 0$ ,  $f$  has a degree, say  $n$ . If  $g - h \neq 0$ , let its degree be  $m$ . Then  $f(g - h)$

is of degree  $n + m$ , which is impossible since the zero polynomial has no degree. Therefore,  $g - h \equiv 0$ , so that  $g \equiv h$ .

**Example 2** To every complex number  $x$  make correspond  $|x|$ . Show that this function of  $x$  is not a polynomial in  $x$ .

Suppose it is a polynomial  $f(x)$ . Since  $f(1) = 1, f \neq 0$ . Let its degree be  $n$ . Since  $f(0) = 0, f$  is not a constant. Hence  $n \geq 1$ . Therefore  $f(x) - 1$  is of degree  $n$  and cannot vanish for infinitely many values of  $x$ . Since  $|x| = 1$  for infinitely many values of  $x$ , we have a contradiction.

### Exercises

- 1 To every complex number  $x$  make correspond one of the square roots of  $x$ . Show that this function is not a polynomial in  $x$ .
- 2 To every complex number  $x = a + bi$  make correspond the real part  $a$ . Show that this function is not a polynomial in  $x$ .
- 3 The conjugate of  $x$  is not a polynomial in  $x$ .
- 4 There is no polynomial  $f(x)$  such that  $f(x) = p$  whenever  $x = p/q$  where  $p$  and  $q$  are integers,  $p$  positive, and the fraction is in its lowest terms.
- 5 If  $f$  and  $1/f$  are polynomials in  $x$ , then  $f$  is a non-zero constant.
- 6 If  $f^2 = 1$  then either  $f = 1$  or  $f = -1$ .
- 7 There exists no polynomial  $f(x)$  such that  $f(x) = |x|$  for every real value of  $x$ .
- 8 If  $f$  and  $g$  are both of degree  $n$ , have the same leading coefficients, and are equal for  $n$  values of  $x$ , then  $f = g$ .
- 9 A function  $f(x)$  is said to be periodic if there exists a number  $h \neq 0$  such that  $f(x + h) \equiv f(x)$ . Prove: A polynomial is not periodic unless it is a constant.
- 10 If  $f(x)$  is a polynomial in  $x, f(|x|)$  is not a polynomial in  $x$  unless  $f(x)$  is a constant.
- 11 Prove: If  $f(x) \equiv f(-x)$ , then the coefficients of the odd powers of  $x$  in  $f(x)$  are zero.
- 12 State and establish a result similar to that in ex. 11 if  $f(x) \equiv -f(-x)$ .
- 13 If  $f(x) \equiv f(2x)$  then  $f(x)$  is a constant.
- 14 If the sum of two polynomials is identical with their product, then each is a constant.
- 15 If  $f^2(x) + g^2(x)$  is a non-zero constant, then  $f$  and  $g$  are constants.
- 16 If  $f(x)$  and  $g(x)$  are polynomials, then  $f(g(x))$  is a polynomial in  $x$  obtained by replacing  $x$  wherever it appears in  $f(x)$  by  $g(x)$ . Prove: If  $f(g(x)) \equiv 0$  then either  $g$  is a constant or  $f \equiv 0$ .

- \*17** Let  $f_0, f_1, \dots, f_n$  be of degrees  $0, 1, \dots, n$  respectively. Prove: If  $F$  is identically zero or of degree at most  $n$ , then  $F$  is uniquely expressible in the form  $c_0 f_0 + c_1 f_1 + \dots + c_n f_n$  where  $c_0, c_1, \dots, c_n$  are constants. (The unique expressibility of a polynomial in the form  $c_0 + c_1 x + \dots + c_n x^n$  is a special case with  $f_0 \equiv 1, f_1 \equiv x, \dots, f_n \equiv x^n$ ).
- 18** If  $x_1, x_2, \dots, x_{n+1}$  are distinct complex numbers, show that constants  $c_0, c_1, \dots, c_n$  can be so determined that  $c_0 + c_1(x - x_1) + c_2(x - x_1)(x - x_2) + \dots + c_n(x - x_1)(x - x_2) \dots (x - x_n)$  shall have the values  $a_1, a_2, \dots, a_{n+1}$  respectively for  $x = x_1, x_2, \dots, x_{n+1}$ . Show also that there is no other polynomial which is identically zero or of degree at most  $n$  which has the values  $a_i$  for  $x = x_i (i = 1, 2, \dots, n+1)$ . (This is called Newton's interpolation formula.)
- 19** Find a formula for  $a_n$  in terms of  $n$  so that  $a_1 = 1^2, a_2 = 2^2, a_3 = 3^2, a_4 = \lambda$ , where  $\lambda$  is any given number. (Thus, it is absurd to say "determine the next number" or "find the general term" when a few numbers at the beginning of a sequence are given.)
- 20** Find a polynomial  $f(x)$  such that  $f(x+1) - f(x) \equiv x^2$ . Hence find  $1^2 + 2^2 + \dots + n^2$ .
- \*21** If  $f(x)$  is a polynomial,  $a$  a complex number,  $\lambda$  a positive number, show that there is an  $M \geq 0$  such that  $|f(x) - f(a)| \leq |x - a|M$  for every  $x$  satisfying  $|x - a| < \lambda$ . Hence show that if  $\epsilon$  is a given positive number there exists a positive number  $\delta$  such that  $|f(x) - f(a)| < \epsilon$  whenever  $|x - a| < \delta$ . (A function with the last property is said to be continuous at  $x = a$ .)

**5. Number fields** With polynomials, as with numbers, the most frequently used operations are addition, multiplication, subtraction, and division (the so-called rational operations). How polynomials behave under these operations depends upon how the coefficients behave. For instance, if it be true that whenever we add or multiply numbers of a certain type we obtain a number of the same type, then it will also be true that whenever we add or multiply polynomials with coefficients of that type we obtain a polynomial with coefficients of the same type.

If we wish to extend the last statement to make it true whenever we perform any of the four rational operations, we should like to consider polynomials whose coefficients are of such a type that

\* Results contained in the starred exercises are used in proving later theorems. Outlines of proofs will be found in Appendix II.

whenever we add, multiply, subtract or divide numbers of that type we obtain a number of the same type. Such a set of numbers is called a field of numbers (briefly, a field) or a domain of rationality. More precisely, a field of numbers is a set of complex numbers such that

- (a) There are at least two numbers in the set
- (b) Whenever  $a$  and  $b$  are in the set then  $a + b$ ,  $a - b$ ,  $ab$  are in the set, and if  $b \neq 0$  then  $a/b$  is also in the set.

The set consisting of the number 0 by itself satisfies (b) but not (a). Thus, requirement (a) rules out this trivial situation.

The rational numbers, that is, the numbers expressible as ratios of integers, form a field. So do the real numbers and the complex numbers. There are other fields besides these, as we shall presently see.

By introducing the idea of a field we can study at once many properties of polynomials concerned with the rational operations regardless of what the coefficients may be as long as they belong to some specified field. Thus, for example, we frequently avoid the necessity of establishing a result for polynomials with rational coefficients and then having to establish it again for polynomials with real coefficients. Furthermore, the result, once established, will apply not only to polynomials with rational coefficients and polynomials with real coefficients but also to polynomials whose coefficients belong to any one of infinitely many different fields.

*Example 1* Do the positive rational numbers form a field?

No, since  $a - b$  may not be a positive rational number when  $a$  and  $b$  are.

*Example 2* Do the numbers of the form  $(a + bi)/(c + di)$ , where  $a, b, c, d$  are integers, form a field?

Yes. We leave it to the reader to verify that the sum, product, difference, and quotient of any two such numbers is a number of the same type.

### Exercises

1 Which of the following sets of numbers are fields?

- a)  $-3, -2, -1, 0, 1, 2, 3$
- b) The non-zero real numbers
- c) The complex numbers of the form  $a + bi$  where  $a$  and  $b$  are integers

- d) The numbers of the form  $a + bi$  where  $a$  and  $b$  are any rational numbers
  - e) The numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are any rational numbers
  - f) The integers
  - g) The numbers of the form  $a + b\sqrt{7}$  where  $a$  and  $b$  are any rational numbers
  - h) The numbers of the form  $a + bi\sqrt{3}$  where  $a$  and  $b$  are any rational numbers
  - i) The numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are any rational numbers
  - j) The numbers of the form  $a + b\sqrt{2} + c\sqrt{3}$  where  $a, b, c$  are any rational numbers.
- \*2 Prove: Every field contains all the rational numbers.
- 3 There are only two fields which contain all the real numbers: (a) the field of all real numbers (b) the field of all complex numbers.
- 4 The numbers common to two fields form a field.
- 5  $\sqrt[3]{3}$  is not in the field (e) of ex. 1.
- 6 A field containing an imaginary cube root of 1 contains all the cube roots of 1.
- 7 If  $\lambda$  is a root of a quadratic equation with rational coefficients, the totality of numbers expressible in the form  $a + b\lambda$ , where  $a$  and  $b$  are rational, form a field. [Exercise 1 (e), (g), (h) are special cases.]
- 8 If  $\lambda$  is given, the numbers expressible in the form  $(a_0\lambda^n + a_1\lambda^{n-1} + \dots + a_{n-1}\lambda + a_n) / (b_0\lambda^m + b_1\lambda^{m-1} + \dots + b_{m-1}\lambda + b_m)$ , where  $m$  and  $n$  are any non-negative integers and the  $a_i$  and  $b_i$  any integers, form a field.
- \*9 If  $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m, \lambda$ , are in the field  $\mathfrak{F}$ , then  $(a_0\lambda^n + a_1\lambda^{n-1} + \dots + a_n) / (b_0\lambda^m + b_1\lambda^{m-1} + \dots + b_m)$  is in  $\mathfrak{F}$ .
- 10 If a set of numbers is such that  $a - b$  is in the set whenever  $a$  and  $b$  are, then  $a + b$  is in the set whenever  $a$  and  $b$  are.

## 6. Division algorithm Let

$$f(x) \equiv a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

$$g(x) \equiv b_0x^m + b_1x^{m-1} + \dots + b_{m-1}x + b_m, \quad b_0 \neq 0$$

If  $n \geq m$  then  $f - (a_0/b_0)x^{n-m}g$  is a polynomial  $f_1$  which is either zero or of degree  $n_1 < n$ .

If  $n_1 \geq m$  and  $f_1 \equiv c_0x^{n_1} + \dots + c_{n_1}$ , then  $f_1 - (c_0/b_0)x^{n_1-m}g$  is a polynomial  $f_2$  which is either zero or of degree  $n_2 < n_1$ .

If  $n_2 \geq m$  we can continue in a similar way, choosing  $a$  so that  $f_2 - ax^{n_2-m}g$  is either zero or of lower degree than  $f_2$ .

Evidently the process can be continued until we obtain a polynomial  $f_k$  which is either zero or of degree less than  $m$ . We then have

$$f \equiv \frac{a_0}{b_0} x^{n-m}g + f_1 \equiv Q_1g + f_1$$

where  $Q_1$  is a polynomial,

$$f \equiv Q_1g + \frac{c_0}{b_0} x^{n_1-m}g + f_2 \equiv Q_2g + f_2$$

where  $Q_2$  is a polynomial and, finally,

$$f \equiv Q_kg + f_k$$

where  $Q_k$  is a polynomial.

The reader will recognize what we have done as exactly the steps in the usual procedure for dividing  $f(x)$  by  $g(x)$ .

We arrived at our final result on the assumption that  $n \geq m$ . If  $n < m$  the final result still holds if we take  $Q \equiv 0$  and  $f_k \equiv f$ .

Thus, in all cases, we have proved:

#### THEOREM

*If  $f$  and  $g$  are given polynomials,  $g \neq 0$ , then  $f \equiv Qg + R$  where  $R$  is either zero or of lower degree than  $g$ .*

We now show:

#### THEOREM

*The  $Q$  and  $R$  of the preceding theorem are unique.*

*Proof:* Suppose  $Qg + R \equiv Q'g + R'$  where each of  $R, R'$  is either zero or of lower degree than  $g$ . Then  $(Q - Q')g \equiv R' - R$  is either zero or of lower degree than  $g$ . But if  $Q - Q' \neq 0$  then the left side has a degree at least as great as that of  $g$ . Hence, we must have  $Q - Q' \equiv 0$  and, therefore, also  $R - R' \equiv 0$ , which proves the theorem.

The  $Q$  and  $R$  are called the quotient and remainder respectively in the division of  $f$  by  $g$ .

We note that in obtaining  $Q$  and  $R$  the only operations performed upon the coefficients of  $f$  and  $g$  are the rational operations.

Hence, if the coefficients of  $f$  and  $g$  lie in a field  $\mathfrak{F}$ , the coefficients of  $Q$  and  $R$  also lie in  $\mathfrak{F}$ .

### Exercises

- Find the quotient and remainder when the first polynomial is divided by the second:
  - $2x^3 + x^2 + x - 1, x^2 + x + 1$
  - $x^3 - 7x - 1, x - 2$
  - $x^4 - 2x^2 - 1, x^2 + 3x - 1$
  - $2x^3 - 3x^2 + 1, x$
  - $x^5 + 7x^4 - 3x^2 + x - 2, x^3 - 3x + 4$
  - $x^2 + x + 1, 2$
  - $3x^2 - x - 1, x^3 - 2$
  - $x^5 + x^4 + 1, x^4 + x^2 + 1$
- Prove: The remainder in the division of  $f(x)$  by  $x - r$  is  $f(r)$ . (This is called the remainder theorem; the factor theorem is a special case in which  $f(r) = 0$ .)
- Find, without actual division, the remainder when the first polynomial is divided by the second:
 

a) $x^3 - x + 4, x - 2$	c) $x^{60} - r, x^{20} - 1$
b) $x^4 - 7x^3 + 5x^2 - x + 1, x + 1$	f) $x^{203} - 1, x^4 - 1$
e) $x^{12} - r^6x^6 + r, x - r$	g) $x^{100} + 1, x^6 + r$
d) $x^{40} - 1, x^4 - 1$	
- Prove: When  $f$  is divided by  $(r - a)(x - b)$  where  $a$  and  $b$  are distinct complex numbers, the remainder is  $x[f(a) - f(b)]/(a - b) + [af(b) - bf(a)]/(a - b)$ .
- If  $g$  is of degree  $n$  and has  $n$  roots and  $f$  vanishes for each of these roots, determine the remainder when  $f$  is divided by  $g$ .
- If the remainder when  $f(x)$  is divided by  $x^2 - 3x + 2$  is  $2x - 3$ , find  $f(1)$  and  $f(2)$ .
- When  $f$  is divided by  $(x^2 - 4)(x + 1)$  the remainder is  $x^2 + 3x + 5$ . What is the remainder when  $f$  is divided by  $x^2 - 4$ ?
- Show that there exists no polynomial which gives the remainders  $x - 5$  and  $2x + 3$  respectively upon division by  $x^2 - 1$  and  $x^2 - 3x + 2$ .
- If the remainder when  $f$  is divided by  $x + 1$  is 3 and the remainder when it is divided by  $(x - 1)^2$  is  $2x + 5$ , find the remainder when  $f$  is divided by  $(x + 1)(x - 1)^2$ .
- If the remainder when  $f$  is divided by  $x^2 + 1$  is  $x$  and the remainder when it is divided by  $x^2 - 1$  is  $2x$ , find the remainder when  $f$  is divided by  $(x^2 + 1)(x^2 - 1)$ .

**7. Divisibility of polynomials** Whether one integer is divisible by another depends upon what kinds of numbers we admit as factors. Thus, 5 is not divisible by 2 if we make the usual requirement that the factors be integers. However, if we admit all rational factors, then 5 is divisible by 2, since  $5 = 2(5/2)$ .

To discuss divisibility of polynomials we must first agree upon a suitable definition. We say polynomial  $f$  is divisible by polynomial  $g$  if  $g \neq 0$  and there exists a polynomial  $h$  such that  $f = gh$ . If  $f$  is divisible by  $g$ , we also say  $g$  divides  $f$ , or  $g$  is a factor of  $f$ , or  $g$  is a divisor of  $f$ .

If  $R = 0$  in the division algorithm  $f = Qg + R$ , then  $g$  divides  $f$ . Conversely, if  $g$  divides  $f$  then  $f = gh$ , so that  $Q = h$  and  $R = 0$ . Thus,  $g$  divides  $f$  if and only if  $R = 0$  in the algorithm. It follows also that if  $f = gh$  then the coefficients of  $h$  lie in every field which contains the coefficients of  $f$  and  $g$ .

If  $f$  is a non-zero polynomial and  $a$  a non-zero constant,  $af$  is called an associate of  $f$ . If  $g$  is a factor of  $f$ , then every associate of  $g$  is a factor of every associate of  $f$ , since  $f = gh$  implies  $af = (bg)(h/b)$  if  $b \neq 0$ . Thus, as far as divisibility properties are concerned, a polynomial and its associates play identical roles.

### Exercises

- 1 By means of the factor theorem, determine whether the first polynomial is a factor of the second:
  - a)  $x - 3$ ,  $x^4 - x^3 - 5x^2 - 4x + 3$
  - d)  $2x - 1$ ,  $2x^3 - 5x^2 - 2x + 2$
  - b)  $x + 1$ ,  $2x^3 - 7x^2 - 4x + 5$ ,
  - e)  $x - 2$ ,  $x^4 - 3x + 2$
  - c)  $x + 2$ ,  $2x^3 - 3x^2 + x + 1$
- 2 For what values of  $k$  is the first polynomial a factor of the second:
  - a)  $x - 1$ ,  $k^2x^3 + 3kx^2 + 2$ ?
  - b)  $x - 2$ ,  $x^4 - 3x^2 + (k + 2)x + k^2 - 16$ ?
  - c)  $x - k$ ,  $x^3 - kx^2 - 2x + k + 3$ ?
  - d)  $x - k + 1$ ,  $x^3 - kx^2 - 2x + k - 3$ ?
  - e)  $x + k$ ,  $x^3 + kx^2 - 2x - 2k + 1$ ?
  - f)  $x + 2k$ ,  $x^4 + 2kx^3 - x^2 - kx + 2k^2$ ?
- 3 For what values of  $k$  and  $l$  is the first polynomial a factor of the second:
  - a)  $x^2 - 3x + 2$ ,  $x^3 - (k + l)x^2 - 2lx$ ?
  - b)  $(x - k)(x - l)$ ,  $x^3 - (2k + l)x^2 + kx$ ?
- 4 Prove:  $f$  and  $g$  are associates if and only if each divides the other.
- 5 Prove: If  $f$  is an associate of  $g$ , then  $g$  is an associate of  $f$ .
- \*6 Prove: If  $f$  is an associate of  $g$  and  $g$  is an associate of  $h$ , then  $f$  is an associate of  $h$ .



**8. Highest common factor** We shall denote by  $\mathfrak{F}[x]$  the set of all polynomials with coefficients in the field  $\mathfrak{F}$ .

Any two polynomials have factors in common, since every non-zero constant is a factor of both. But they may or may not have other common factors. What factors they have in common depends upon what domain  $\mathfrak{F}[x]$  we require the factors to lie in.

For example, if  $f \equiv x^4 + x^3 + 3x^2 + 2x + 2$  and  $g \equiv x^4 + 3x^2 + 2$ , then

- (a) If  $\mathfrak{F}$  is the field of complex numbers,  $f$  and  $g$  have  $i$ ,  $x + i\sqrt{2}$ ,  $x - i\sqrt{2}$ ,  $x^2 + 2$  as common factors,
- (b) If  $\mathfrak{F}$  is the field of real numbers, only  $x^2 + 2$  of the previous four is a common factor.

If  $f$  and  $g$  are in  $\mathfrak{F}[x]$ , it would be convenient to be able to speak of a common factor in  $\mathfrak{F}[x]$  which in some sense includes all their common factors in  $\mathfrak{F}[x]$ . For this purpose we define a polynomial  $D$  in  $\mathfrak{F}[x]$  to be a highest common factor of  $f$  and  $g$  over  $\mathfrak{F}$  (abbreviated H.C.F.) if it is a common factor which is divisible by every common factor in  $\mathfrak{F}[x]$ .

We show, by means of the so-called Euclidean algorithm, that if  $f$  and  $g$  are in  $\mathfrak{F}[x]$ , not both zero, a H.C.F. in  $\mathfrak{F}[x]$  exists. The algorithm provides a method for obtaining such a H.C.F.

Suppose  $g \neq 0$ . For convenience in notation denote  $f$  by  $R_0$  and  $g$  by  $R_1$ .

By the division algorithm,  $R_0 \equiv Q_1R_1 + R_2$  where  $R_2$  is either zero or of lower degree than  $R_1$ .

If  $R_2 \neq 0$  then similarly  $R_1 \equiv Q_2R_2 + R_3$  where  $R_3$  is zero or of lower degree than  $R_2$ .

The process may be continued as long as the remainder obtained is not the zero polynomial. But, since the degrees of the remainders keep diminishing and can never become negative, the process cannot continue indefinitely. That is, the zero polynomial must eventually be obtained as a remainder.

If  $R_0, R_1, \dots, R_k$  are non-zero and  $R_{k+1}$  is zero, the algorithm is

$$\begin{array}{rcl} R_0 & \equiv & Q_1R_1 + R_2 \\ R_1 & \equiv & Q_2R_2 + R_3 \\ & \cdot & \cdot \cdot \cdot \cdot \cdot \\ R_{i-1} & \equiv & Q_iR_i + R_{i+1} \\ & \cdot & \cdot \cdot \cdot \cdot \cdot \end{array}$$

$$\begin{aligned}R_{k-2} &\equiv Q_{k-1}R_{k-1} + R_k \\ R_{k-1} &\equiv Q_k R_k\end{aligned}$$

We say that  $R_k$  is a H.C.F. of  $R_0$  and  $R_1$  over  $\mathfrak{F}$ .

If  $\mathfrak{F}$  is a field containing the coefficients of  $f$  and  $g$ , then all the quotients and remainders are in  $\mathfrak{F}[x]$ . Thus, the coefficients of  $R_k$  lie in every field which contains the coefficients of  $f$  and  $g$ .

The last line of the algorithm shows that  $R_k$  is a factor of  $R_{k-1}$ . Since  $R_k$  is a factor of  $R_k$  and  $R_{k-1}$ , the next to last line shows that it is also a factor of  $R_{k-2}$ . Working up the algorithm, we see successively that  $R_k$  is a factor of  $R_{k-1}$ ,  $R_{k-2}$ ,  $\dots$ ,  $R_{i+1}$ ,  $R_i$ ,  $R_{i-1}$ ,  $\dots$ ,  $R_1$ ,  $R_2$ ,  $R_1$ ,  $R_0$ .

Thus,  $R_k$  is a common factor of  $R_0$  and  $R_1$ .

If  $Q$  is any common factor of  $R_0$  and  $R_1$ , the first line  $R_2 = R_0 - Q_1 R_1$  shows that  $Q$  is a factor of  $R_2$ . From the second equality  $R_3 \equiv R_1 - Q R_2$  we see that it is a factor of  $R_3$ . Working down the algorithm we see finally that  $Q$  is a factor of  $R_k$ .

Thus, by definition of a H.C.F.,  $R_k$  is a H.C.F. of  $R_0$  and  $R_1$  over  $\mathfrak{F}$ .

If a polynomial is a H.C.F. of  $f$  and  $g$  over *any* field which contains the coefficients of  $f$  and  $g$ , we generally refer to it merely as a H.C.F., omitting mention of any field. We have seen that  $R_k$  is such a H.C.F.

*Example* Let  $R_0 = x^6 - 6x^4 + 11x^2 - 342$ ,  $R_1 = x^3 - 3x^2 - 4x + 12$ .

The Euclidean algorithm is

$$\begin{aligned}R_0 &= (x^3 + 3x^2 + 7x + 21)R_1 + 66(x^2 - 9) \\ R_1 &\equiv -\frac{x-3}{66} R_2 + 5(x-3) \\ R_2 &\equiv \frac{66}{5}(x+3)R_3\end{aligned}$$

Thus,  $5(x-3)$  is a H.C.F. It follows (ex. 1, §9) that  $x-3$  is also a H.C.F.

*Remark* If, at any stage of the Euclidean algorithm, instead of applying the division algorithm to  $R_{i-1}$  and  $R_i$  we apply it to  $aR_{i-1}$  and  $bR_i$ , where  $a$  and  $b$  are non-zero constants in  $\mathfrak{F}$ , the only effect on the final remainder is to alter it by a non-zero constant factor in  $\mathfrak{F}$ . This, however, does not change the fact that the final remainder is a H.C.F. over  $\mathfrak{F}$  (ex. 1, §9).

Thus, in the example the cumbersome fractional coefficients may be avoided as follows: Dividing  $R_1$  by  $x^2 - 9$  instead of by  $66(x^2 - 9)$ ,  $R_1 \equiv (x - 3)(x^2 - 9) + 5(x - 3)$ . Then, dividing by  $x - 3$  instead of by  $5(x - 3)$ ,  $x^2 - 9 \equiv (x + 3)(x - 3)$ . Hence,  $x - 3$  is a H.C.F.

## 9. Form for H.C.F.

### THEOREM

If  $R_k$  is the H.C.F. of  $f$  and  $g$  obtained by the Euclidean algorithm, then  $R_k \equiv Af + Bg$  where  $A$  and  $B$  are polynomials whose coefficients lie in every field which contains the coefficients of  $f$  and  $g$ .

*Proof:* We show that every one of the  $R_i$  is expressible in this form.

For  $R_0$  and  $R_1$  this is obvious with  $A \equiv 1$ ,  $B \equiv 0$  and  $A \equiv 0$ ,  $B \equiv 1$  respectively.

If  $R_{i-1} \equiv A_{i-1}f + B_{i-1}g$  and  $R_i \equiv A_i f + B_i g$ , then

$$\begin{aligned} R_{i+1} \equiv R_{i-1} - Q_i R_i &\equiv (A_{i-1}f + B_{i-1}g) \\ &\quad - Q_i(A_i f + B_i g) \equiv A_{i+1}f + B_{i+1}g \end{aligned}$$

where  $A_{i+1} \equiv A_{i-1} - Q_i A_i$ ,  $B_{i+1} \equiv B_{i-1} - Q_i B_i$ .

Thus, proceeding by successive steps down the algorithm, we see finally that  $R_k$  is expressible in the desired form.

### Exercises

- 1 If  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ , then every associate of  $D$  in  $\mathfrak{F}[x]$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ .
- 2 Any two H.C.F.'s of  $f$  and  $g$  over  $\mathfrak{F}$  are associates.
- 3 A H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$  is a H.C.F. over  $\mathfrak{F}$  of any associates of  $f$  and  $g$  in  $\mathfrak{F}[x]$ .
- 4 Find a H.C.F. for each of the following pairs of polynomials:
  - a)  $x^6 + 7x^5 + 17x^4 + 18x^3 + 13x^2 + 12x + 6$ ,  
 $x^6 + 4x^4 + 4x^3 + 3x^2 + 3x + 1$
  - b)  $x^5 + x^4 + 1$ ,  $x^4 + x^2 + 1$
  - c)  $x^6 + 2x^4 - 3x^2 - 2x + 2$ ,  $2x^4 + x^3 - 4x^2 + 1$
  - d)  $2x^4 - x^3 - 8x^2 + 3x - 2$ ,  $6x^4 - 3x^3 - 16x^2 + x + 2$
  - e)  $2x^3 + x^2 - 9$ ,  $3x^4 + 6x^3 + 8x^2 - 2x - 3$
  - f)  $x^5 - 2x^3 - 3x^2 + 6$ ,  $x^4 + x^3 - x^2 - 2x - 2$
  - g)  $4x^3 + 16x^2 - 9x - 36$ ,  $2x^3 - x^2 - 22x - 24$

- h)  $x^3 - 6x^2 + 3x - 4$ ,  $x^3 - 15x - 28$   
 i)  $8x^5 + 20x^4 - 10x^3 - 45x^2 + 27$ ,  $4x^4 + 8x^3 - 3x^2 - 9x$
- 5 If  $\mathfrak{F}$  is the field of real numbers and  $r$  is in  $\mathfrak{F}$ , then  $x^4 - 10x^2 + r^2x$  and  $x^2 - x + r^2$  have a common factor in  $\mathfrak{F}[x]$  other than a constant if and only if  $r = 0$ .
  - 6  $2x^3 + 5x^2 + 3x - r$  and  $x^3 + 2x^2 + 4x - r$  have no common quadratic factor in  $\mathfrak{F}[x]$  where  $\mathfrak{F}$  is any field containing the coefficients.
  - 7 If  $x^3 + x^2 - ax + b$ ,  $x^3 + 2x^2 + bx - a$  have a common quadratic factor, find  $a$  and  $b$ .
  - 8 Determine  $r$  so that  $x^4 - x^3 - 5x^2 - 8x - 2$  and  $x^3 + 3x^2 + 4x + r$  shall have a common quadratic factor.
  - 9 If  $f$  and  $g$  are distinct polynomials in  $\mathfrak{F}[x]$ , then a H.C.F. of  $f + g$  and  $f - g$  over  $\mathfrak{F}$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ , and conversely.
  - 10 Let  $f$ ,  $g$ ,  $D$  be in  $\mathfrak{F}[x]$ ,  $D$  a common factor of  $f$  and  $g$ . Then  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$  if and only if  $f$  and  $g$  have no common factor in  $\mathfrak{F}[x]$  of higher degree than  $D$ .
  - 11 If  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ , it is a H.C.F. of  $f$  and  $g$  over every field which contains the coefficients of all three polynomials.
  - 12 Let  $f$ ,  $g$ ,  $D$  be in  $\mathfrak{F}[x]$ ,  $D$  a common factor of  $f$  and  $g$ . Then  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$  if and only if  $D \equiv Af + Bg$  where  $A$  and  $B$  are in  $\mathfrak{F}[x]$ .
  - 13 For each of the pairs of polynomials  $f$  and  $g$  in ex. 4 find  $A$  and  $B$  so that  $Af + Bg$  shall be a H.C.F.
  - 14 If  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$  and  $h \neq 0$  is in  $\mathfrak{F}[x]$ , then  $Dh$  is a H.C.F. of  $fh$  and  $gh$  over  $\mathfrak{F}$ .
  - 15 If  $D(x)$  is a H.C.F. of  $f(x)$  and  $g(x)$  over  $\mathfrak{F}$  and  $n$  is a positive integer, then  $D(x^n)$  is a H.C.F. of  $f(x^n)$  and  $g(x^n)$  over  $\mathfrak{F}$ .
  - 16 If  $f$  and  $g$  are in  $\mathfrak{F}[x]$ ,  $g \neq 0$ , consider all polynomials expressible in the form  $Af + Bg$  where  $A$  and  $B$  are in  $\mathfrak{F}[x]$ . Let  $D$  be one of these of lowest degree. Prove  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ .
  - 17 Define a H.C.F. of  $f$ ,  $g$ ,  $h$  over  $\mathfrak{F}$ . If  $h \neq 0$  show that one exists and describe a method for obtaining it. Extend this to any number of polynomials.

**10. Relatively prime polynomials** If  $f$  and  $g$  are non-zero polynomials in  $\mathfrak{F}[x]$ , they are said to be relatively prime, or prime to each other, over  $\mathfrak{F}$  if their only common factors in  $\mathfrak{F}[x]$  are constants. In this case  $R_k$  in the Euclidean algorithm is a non-zero constant in  $\mathfrak{F}$ . From  $R_k \equiv Af + Bg$  we obtain, by dividing by  $R_k$ ,  $1 \equiv A'f + B'g$  where  $A'$  and  $B'$  are polynomials whose coefficients lie in every field which contains the coefficients of  $f$  and  $g$ .

If  $\mathfrak{F}'$  is any other field containing the coefficients of  $f$  and  $g$ , and  $C$  any common factor of  $f$  and  $g$  in  $\mathfrak{F}'[x]$ , then  $C$ , being a factor of  $Af + Bg$ , is a factor of 1 and, therefore, a constant. Thus,  $f$  and  $g$  are relatively prime over  $\mathfrak{F}'$ .

Thus, if  $f$  and  $g$  are relatively prime over one field they are relatively prime over every field which contains their coefficients. For this reason we generally speak of polynomials being relatively prime without referring to any specific field.

### Exercises

- 1 Determine whether the following pairs of polynomials are relatively prime:
  - a)  $x^2 + 1, x^3 + x^2 + 2$
  - b)  $x - 2, 2x^4 - x + 1$
  - c)  $x^2 - x + 1, 2x^4 - x^3 - x^2 + 3x - 2$
  - d)  $2x^3 - x^2 - 5x - 2, x^3 + x^2 - 2x$
  - e)  $2x^4 - x^3 - 3x^2 + 2x - 2, x^5 - x^3 + x^2 - 2x - 2$
  - f)  $x^4 + 3x^3 + 2x^2 - x + 3, x^5 + 2x^2 + 1$
- 2 If  $f = AF \neq 0, g = AG \neq 0$ , where  $A, F, G$  are in  $\mathfrak{F}[x]$ , then  $A$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$  if and only if  $F$  and  $G$  are relatively prime.
- 3 If  $f$  and  $g$  are relatively prime, they have no common root.
- 4 If  $f$  and  $g$  are relatively prime, every associate of  $f$  is prime to every associate of  $g$ .
- \*5 If  $f$  and  $g$  are relatively prime,  $n$  and  $m$  positive integers, then  $f^n$  and  $g^m$  are relatively prime. (Hint: First show  $f^n, g$  relatively prime.)
- 6 If  $D$  is a H.C.F. of  $f$  and  $g$  over  $\mathfrak{F}$ , then  $D^n$  is a H.C.F. of  $f^n$  and  $g^n$  over  $\mathfrak{F}$ . (Hint: Use exs. 2, 5.)
- 7 If  $h$  is prime to  $f$  and  $g$ , it is prime to  $fg$ . Extend this to the product of any number of polynomials.
- 8 If  $f$  is divisible by  $g$  and by  $h$ , and  $g$  and  $h$  are relatively prime, then  $f$  is divisible by  $gh$ . Show by an example that the conclusion may not follow if  $g$  and  $h$  are not relatively prime.
- \*9 If  $fg$  is divisible by  $h$ , and  $f$  and  $h$  are relatively prime, then  $g$  is divisible by  $h$ . Extend this to the product of any number of polynomials. Show by an example that the conclusion may not follow if  $f$  and  $h$  are not relatively prime.
- \*10 If  $Af + Bg = 0$ , where  $f$  is of degree  $n$  and  $B$  of degree  $n - p$  or less, then  $f$  and  $g$  have a common factor of degree at least  $p$ .

**11. Irreducible polynomials** If  $f$  is in  $\mathfrak{F}[x]$  and  $c$  is a non-zero constant in  $\mathfrak{F}$ , then  $f$  is divisible by  $c$ . If  $f$  is itself a constant, there

are no other divisors of  $f$  in  $\mathfrak{F}[x]$ . But if  $f$  is not a constant there may be polynomials  $g$  and  $h$  in  $\mathfrak{F}[x]$ , neither a constant, such that  $f \equiv gh$ . If this is so,  $f$  is said to be reducible or composite over  $\mathfrak{F}$ . If, however,  $f$  is not constant and  $f \equiv gh$ , where  $g$  and  $h$  are in  $\mathfrak{F}[x]$ , implies that one of  $g$  and  $h$  is a constant (and the other then is an associate of  $f$ ), then  $f$  is said to be irreducible, indecomposable, or prime over  $\mathfrak{F}$ .

For example,  $f \equiv x^2 + 6x + 7$  is:

- (a) Reducible over the field of real numbers, since  $f \equiv (x + 3 + \sqrt{2})(x + 3 - \sqrt{2})$  and neither of the factors is a constant.
- (b) Irreducible over the field of rational numbers. For if  $f \equiv gh$  where  $g$  and  $h$  have rational coefficients and neither is a constant, then  $g$  and  $h$  are of degree one or more. If either were of degree higher than one, the degree of the product would exceed two. Therefore, each is of degree one. If  $g \equiv ax + b$ ,  $a \neq 0$ , then  $-\frac{b}{a}$  is a rational root of  $g$  and therefore also of  $f$ . But neither of the roots  $-3 \pm \sqrt{2}$  of  $f$  is rational.

Evidently, as this example shows, a polynomial may be reducible over one field and irreducible over another.

### Exercises

- 1 Show that the following polynomials are reducible over the given fields:
  - a)  $x^4 + 4x^2 + 3$ , rational numbers
  - b)  $x^4 + 1$ , numbers of the form  $a + bi$  where  $a$  and  $b$  are rational
  - c)  $x^3 - 2x + 1$ , rational numbers
  - d)  $x^4 - 2x^2 - 1$ , real numbers
  - e)  $x^2 + x - 1$ , numbers of the form  $a + b\sqrt{5}$  where  $a$  and  $b$  are rational
  - f)  $2x^3 + x^2 + x - 1$ , rational numbers
- 2 Show that the following are irreducible over the given fields:
  - a)  $x^3 - 2$ , rational numbers
  - b)  $x^2 - 4x + 2$ , rational numbers
  - c)  $x^4 - 6x^2 + 13$ , real numbers
  - d)  $x^2 - 3$ , numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are rational
  - e)  $x^5 - 7$ , rational numbers
- 3 If  $r$  is a real number,  $\mathfrak{F}$  the field of real numbers,  $x^2 + rx + r^2$  is reducible over  $\mathfrak{F}$  if and only if  $r = 0$ .

- 4 If  $r$  is an integer,  $\mathfrak{F}$  the field of rational numbers, then
  - a)  $x^2 + (r + 1)x + r$  is reducible over  $\mathfrak{F}$
  - b)  $x^2 + 4rx + 1$  is irreducible over  $\mathfrak{F}$ .
- 5 Every linear polynomial in  $\mathfrak{F}[x]$  is irreducible over  $\mathfrak{F}$ .
- 6 If  $f$  is irreducible over  $\mathfrak{F}$  and has a root in  $\mathfrak{F}$ , then  $f$  is linear.
- 7 If a cubic polynomial is reducible over  $\mathfrak{F}$ , it has a root in  $\mathfrak{F}$ .
- 8 If  $f(x)$  and  $g(x)$  are in  $\mathfrak{F}[x]$  and  $f(g(x))$  is irreducible over  $\mathfrak{F}$ , then  $f$  is irreducible over  $\mathfrak{F}$ .
- \*9 If  $f$  is irreducible over  $\mathfrak{F}$ , every associate of  $f$  in  $\mathfrak{F}[x]$  is irreducible over  $\mathfrak{F}$ .
- 10 If  $f$  is irreducible over  $\mathfrak{F}$  and  $g \neq 0$  is in  $\mathfrak{F}[x]$ , then either  $f$  is prime to  $g$  or  $f$  is a factor of  $g$ .
- \*11 If  $f$  and  $g$  are irreducible over  $\mathfrak{F}$ , they are either prime to each other or they are associates.
- 12  $f$  is irreducible over  $\mathfrak{F}$  if and only if it is prime to every polynomial in  $\mathfrak{F}[x]$  of lower degree than  $f$ .
- \*13 If  $f, f_1, \dots, f_n$  are in  $\mathfrak{F}[x]$ ,  $f$  irreducible over  $\mathfrak{F}$ , and  $f$  divides  $f_1 f_2 \dots f_n$ , then  $f$  divides at least one of  $f_1, f_2, \dots, f_n$ . (Hint: Use ex. 9, §10)

**12. Factorization into primes** If  $f$  is reducible over  $\mathfrak{F}$  then  $f \equiv gh$  where neither  $g$  nor  $h$  is a constant. Therefore, both  $g$  and  $h$  are of lower degree than  $f$ . If either  $g$  or  $h$  is reducible, we may continue the factorization and obtain other factors of still lower degrees. This can be continued as long as we get factors which are not primes. But, since at each stage we obtain polynomials of lower degree than before and the degree of a polynomial is positive or zero, the process cannot continue indefinitely. We must, therefore, eventually reach a stage where  $f \equiv f_1 f_2 \dots f_n$  and each of the factors is irreducible over  $\mathfrak{F}$ .

To illustrate, let  $f \equiv x^6 + 4x^4 + x^2 - 6$ ,  $\mathfrak{F}$  the field of real numbers. This is reducible over  $\mathfrak{F}$  since  $f \equiv (x^4 + x^2 - 2)(x^2 + 3)$ . The second factor  $x^2 + 3$  is irreducible, but the first factor is reducible, and by factoring it we obtain  $f \equiv (x^2 - 1)(x^2 + 2)(x^2 + 3)$ . The last two factors are now irreducible, but the first is not. Continuing the factorization,  $f \equiv (x - 1)(x + 1)(x^2 + 2)(x^2 + 3)$ . All the factors are now irreducible over  $\mathfrak{F}$ .

These remarks lead to the following theorem.

## THEOREM

*A non-constant polynomial in  $\mathfrak{F}[x]$  is either prime over  $\mathfrak{F}$  or a product of polynomials each of which is prime over  $\mathfrak{F}$ .*

*Proof:* Since a linear polynomial cannot be the product of two polynomials each of degree one or more, a linear polynomial in  $\mathfrak{F}[x]$  is prime over  $\mathfrak{F}$ . Therefore, the theorem is valid for polynomials of degree one.

Proceeding by mathematical induction, suppose the desired result established for polynomials of degree  $1, 2, \dots, k$ . Let  $f$  be of degree  $k + 1$ .

If  $f$  is irreducible over  $\mathfrak{F}$ , there is nothing more to be proved.

If  $f$  is reducible, then  $f = gh$  where  $g$  and  $h$  are in  $\mathfrak{F}[x]$  and each is of degree less than  $k + 1$ . By the hypothesis of the induction applied to  $g$  and  $h$ ,  $f$  is a product of polynomials irreducible over  $\mathfrak{F}$ .

By the principle of mathematical induction, the theorem is proved.

Factorization of a polynomial into primes can be accomplished in more than one way. For we can introduce a non-zero constant multiplier into one of the prime factors and compensate for it in some other factor; this does not alter the fact that the factors are primes.

For instance, in the example above, we also have  $f = (2x - 2)(x + 1)(\frac{1}{2}x^2 + 1)(x^2 + 3)$ .

The second factorization, however, is not essentially different from the first, since in the second the factors are associates of those in the first. If we regard such factorizations as the "same," then we do have unique factorization, as the following theorem shows.

## THEOREM

*If  $P_1P_2 \cdots P_l = Q_1Q_2 \cdots Q_m$ , where each of the  $P$ 's and  $Q$ 's is irreducible over  $\mathfrak{F}$ , then  $l = m$  and we can number the  $Q$ 's in such a way that, for each  $i$ ,  $P_i$  and  $Q_i$  are associates.*

*Proof:* If  $l = 1$  then  $P_1 \equiv Q_1 \cdots Q_m$  is a prime over  $\mathfrak{F}$ . Hence  $m = 1$ ,  $P_1 \equiv Q_1$ .

The proof is similar if  $m = 1$ .

Hence suppose  $l > 1$ ,  $m > 1$  and proceed by mathematical induction on  $l$ , supposing the desired result established when there are  $l - 1$  or fewer  $P$ 's.



Since  $P_l$  divides  $Q_1 Q_2 \cdots Q_m$ , it divides some  $Q$  (ex. 13, §11), say  $Q_m$ . Then  $P_l$  and  $Q_m$  are associates (ex. 11, §11). If  $Q_m \equiv \epsilon P_l$ ,  $\epsilon$  a constant in  $\mathfrak{F}$ , then

$$\begin{aligned} P_1 P_2 \cdots P_l &\equiv Q_1 \cdots Q_{m-1} (\epsilon P_l) \\ P_1 \cdots P_{l-1} &\equiv (\epsilon Q_1) Q_2 \cdots Q_{m-1} \quad (\text{cancellation law of example 1,} \\ &\qquad\qquad\qquad \S 4) \\ &\equiv Q'_1 Q_2 \cdots Q_{m-1} \end{aligned}$$

where  $Q'_1$  is a prime over  $\mathfrak{F}$  (ex. 9, §11).

By the hypothesis of the induction  $l-1 = m-1$ , so that  $l = m$ , and  $P_1, \dots, P_{l-1}$  are associates of  $Q'_1, Q_2, \dots, Q_{m-1}$  in some order.

Since an associate of  $Q'_1$  is also an associate of  $Q_1$  (ex. 6, §7), the desired result is established.

By the principle of mathematical induction the theorem is proved.

If we restrict ourselves to primes with leading coefficient 1, then:

#### THEOREM

*A non-constant polynomial in  $\mathfrak{F}[x]$  is uniquely expressible in the form  $aP_1 P_2 \cdots P_n$  where  $a$  is a constant and each  $P_i$  is prime over  $\mathfrak{F}$  and has leading coefficient 1.*

If we combine like factors we have:

#### THEOREM

*A non-constant polynomial in  $\mathfrak{F}[x]$  is uniquely expressible in the form  $aP_1^{r_1} P_2^{r_2} \cdots P_k^{r_k}$  where  $a$  is a constant, the  $r_i$ 's are positive integers, each  $P_i$  is prime over  $\mathfrak{F}$  and has leading coefficient 1, and the  $P_i$ 's are all distinct.*

In a vacuous way, i.e., with no primes, the last two theorems hold also for non-zero constant polynomials.

#### Exercises

1 Factor into primes over the given field:

- $x^4 - 5x^2 + 6$ , rational numbers
- $x^4 - 5x^2 + 6$ , real numbers
- $x^4 - 5x^2 + 6$ ; numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are rational
- $x^4 - 5x^2 + 6$ , complex numbers
- $x^6 - 2x^3 + 1$ , rational numbers

- f)  $x^6 - 2x^3 + 1$ , real numbers
  - g)  $x^6 - 2x^3 + 1$ , complex numbers
  - h)  $x^3 + x^2 + x + 1$ , rational numbers
  - i)  $x^3 + x^2 + x + 1$ , real numbers
  - j)  $x^3 + x^2 + x + 1$ , complex numbers
  - k)  $x^4 + 5x^2 + 2$ , rational numbers
  - l)  $x^4 + 5x^2 + 2$ , real numbers
- 2 If  $f \equiv aP_1^{r_1}P_2^{r_2} \cdots P_k^{r_k}$ , where the  $P$ 's are distinct primes over  $\mathcal{F}$  with leading coefficient 1 and  $a$  is a non-zero constant in  $\mathcal{F}$ , then  $g \neq 0$  in  $\mathcal{F}[x]$  is a factor of  $f$  if and only if  $g \equiv bP_1^{s_1}P_2^{s_2} \cdots P_k^{s_k}$  where  $b$  is a constant and  $0 \leq s_i \leq r_i$ .
- 3 Let  $f \equiv aP_1^{r_1}P_2^{r_2} \cdots P_k^{r_k}$ ,  $g \equiv bP_1^{s_1}P_2^{s_2} \cdots P_k^{s_k}$ , the  $P$ 's distinct primes over  $\mathcal{F}$  with leading coefficient 1,  $a$  and  $b$  non-zero constants in  $\mathcal{F}$ , the  $r$ 's and  $s$ 's non-negative integers. Let  $t_i$  be the smaller of  $r_i$  and  $s_i$ . Prove that  $P_1^{t_1}P_2^{t_2} \cdots P_k^{t_k}$  is a H.C.F. of  $f$  and  $g$  over  $\mathcal{F}$ .
- 4 Prove:  $f$  and  $g$  are relatively prime over  $\mathcal{F}$  if and only if their factorizations into primes over  $\mathcal{F}$  have no prime in common, assuming each prime has leading coefficient 1.

**13. Factorization of integers** Essentially, the entire discussion of factorization of polynomials stemmed from the existence of the division algorithm (§6). We show that a similar algorithm exists for integers and, therefore, a similar factorization theory.

#### THEOREM

If  $k$  and  $n$  are integers,  $n \neq 0$ , there exist integers  $q$  and  $r$  such that  $k = qn + r$  where  $0 \leq r < |n|$ .

*Proof:* If  $k$  is an integral multiple of  $n$ , the desired result is obvious, with  $r = 0$ . Suppose, therefore,  $k$  is not an integral multiple of  $n$ .

Let  $m = |n|$ .

If  $k > 0$ , let  $(q+1)m$  be the first of  $0m, 1m, 2m, \dots$  which exceeds  $k$ . Then  $qm < k < (q+1)m$ , so that  $0 < k - qm < m$ . If  $r = k - qm$ , then  $k = qm + r = q|n| + r = (\pm q)n + r$ , which establishes the desired result in this case.

If  $k < 0$  and  $-k = qm + r$ , where  $0 < r < m$ , then  $k = -qm - r = -qm - m + (m - r) = -(q+1)m + (m - r) = \pm(q+1)n + r'$  where  $0 < m - r = r' < m = |n|$ , which establishes the theorem in this case.

*Remark* Actually there is only one such pair  $q$  and  $r$  (proof left to reader). We shall not, however, need this fact.

From the similarity of this result to the theorem of §6, we see that the absolute value of an integer plays the same role in the theory of factorization of integers that the degree of a polynomial plays in the corresponding theory for polynomials.

In §7 we defined a polynomial  $f$  to be divisible by a polynomial  $g \neq 0$  if  $f \equiv gh$  where  $h$  is a polynomial. Similarly, an integer  $n$  is said to be divisible by an integer  $m \neq 0$  if  $n = mq$  where  $q$  is an integer.

Just as we noted that the non-zero constants are the polynomials which divide all polynomials, we note similarly that 1 and  $-1$  are the integers which divide all integers. Thus, 1 and  $-1$  play the same role in the factorization of integers that the non-zero constants do in the corresponding theory for polynomials. For instance, we define non-zero integers  $m$  and  $n$  as associates if  $m = n$  or  $m = -n$ . Exercises 4, 5, 6 of §7 then apply to integers.

A H.C.F. for integers is defined, as for polynomials (§8), as a common factor which is divisible by every common factor. It then follows, as in §8, that there exists a Euclidean algorithm for determining a H.C.F.  $d$  for any two integers  $m$  and  $n$ , not both zero, and, as in §9, that  $d = am + bn$  where  $a$  and  $b$  are integers.

It follows also that if  $m$  and  $n$  are non-zero relatively prime integers, i.e., with only 1 and  $-1$  as common factors, then there exist integers  $a$  and  $b$  such that  $am + bn = 1$ . Exercise 9, §10 (also, for later use, ex. 5) also applies to integers.

Paraphrasing the definition of a prime polynomial in §11, we say integer  $m \neq 0, 1, -1$  is a prime if  $m = rs$ , where  $r$  and  $s$  are integers, implies that  $r$  or  $s$  is 1 or  $-1$ . Exercises 9, 11, and 13, §11, then apply to integers.

We can now obtain, as in §12, a unique factorization theorem for integers. If we use only positive primes, we have.

### THEOREM

*An integer different from 0, 1, and  $-1$  is uniquely expressible in the form  $ap_1p_2 \cdots p_n$  where the  $p$ 's are positive prime integers and  $a$  is 1 or  $-1$ .*

### Exercises

- 1 A non-zero rational number is uniquely expressible in the form  $m/n$  where  $m$  and  $n$  are relatively prime integers and  $n$  is positive. (When so expressed the fraction is said to be in its lowest terms.)

- 2 There are infinitely many positive prime integers. (Hint: If  $p_1, p_2, \dots, p_n$  were all the positive primes, consider  $p_1 p_2 \cdots p_n + 1$ .)
- 3 If  $q$  is a positive integer which is not the  $n$ th power of a positive integer, where  $n$  is a positive integer, then  $\sqrt[n]{q}$  is irrational.
- 4 Let  $\omega \neq 1$  be an  $n$ th root of 1,  $\omega^d$  the smallest positive power of  $\omega$  which equals 1. Show  $d$  is a factor of  $n$ . (Hint: let  $n = qd + r$ ,  $0 \leq r < n$ , and show  $\omega^r = 1$ .)
- \*5 If  $\omega \neq 1$  is a  $p$ th root of 1,  $p$  a positive prime integer, show that  $\omega^0 = 1, \omega, \omega^2, \dots, \omega^{p-1}$  are distinct and are all the  $p$ th roots of 1. From this show that if  $\alpha$  is a  $p$ th root of  $a \neq 0$ , then  $\alpha, \alpha\omega, \alpha\omega^2, \dots, \alpha\omega^{p-1}$  are distinct and are all the  $p$ th roots of  $a$ .
- \*6 If  $r$  is a factor of  $a_1 a_2 \cdots a_n$ , then  $r = b_1 b_2 \cdots b_n$  where  $b_i$  is a factor of  $a_i$  ( $i = 1, 2, \dots, n$ ).

## POLYNOMIALS IN THE COMPLEX DOMAIN

In this chapter, unless otherwise stated we shall be considering polynomials whose coefficients may be any complex numbers.

**1. Factorization into linear factors** Since the complex numbers form a field, every non-constant polynomial is the product of a constant and irreducible polynomials with leading coefficient 1 (§12, Ch. 2). For further knowledge concerning the nature of the factorization we must determine, if possible, what polynomials are irreducible.

We have already seen (§12, Ch. 2) that every linear polynomial is irreducible.

A quadratic polynomial  $f = a_0x^2 + a_1x + a_2$ ,  $a_0 \neq 0$ , is necessarily reducible, since

$$f = a_0 \left( x + \frac{a_1 + \sqrt{a_1^2 - 4a_0a_2}}{2a_0} \right) \left( x + \frac{a_1 - \sqrt{a_1^2 - 4a_0a_2}}{2a_0} \right)$$

We shall see (Ch. 8) that every cubic and every quartic also has a root in the complex domain. By the factor theorem, therefore, all third and fourth degree polynomials are reducible.

Whether the same is true for polynomials of higher degree is far from obvious. It is a fact, however, that every non-constant polynomial has at least one root. This remarkable result is known as the fundamental theorem of algebra. Its proof depends upon methods generally considered to be outside the domain of algebra, belonging rather to the domain of analysis in which the concept of limit plays a fundamental role. We shall not give a proof here, but we shall use the theorem whenever convenient.

It follows from the fundamental theorem and the factor theorem that every polynomial of degree one or more is reducible. Thus,

the only polynomials irreducible over the complex field are the linear polynomials.

By the unique factorization theorem (§12, Ch. 2) it follows that a polynomial of degree  $n \geq 1$  is the product of a constant and  $n$  linear polynomials with leading coefficient 1. If, for convenience, we express these linear polynomials in the form  $x - r$ , we have:

### THEOREM

*If  $f(x)$  is of degree  $n \geq 1$  it is uniquely expressible in the form  $a(x - r_1)(x - r_2) \cdots (x - r_n)$  where  $a$  is a constant.*

If we combine like factors, we have:

### THEOREM

*If  $f(x)$  is of degree  $n \geq 1$  it is uniquely expressible in the form  $a(x - s_1)^{m_1}(x - s_2)^{m_2} \cdots (x - s_k)^{m_k}$  where  $s_1, s_2, \dots, s_k$  are distinct complex numbers,  $a$  is a constant, and  $m_1, m_2, \dots, m_k$  are positive integers whose sum is  $n$ .*

These theorems hold also in a vacuous way, i.e., with no linear factors, if  $n = 0$ .

**2. Multiplicity of roots** Let  $f(x) \equiv a(x - s_1)^{m_1}(x - s_2)^{m_2} \cdots (x - s_k)^{m_k}$ ,  $a \neq 0$ . Since  $f(x) = 0$  if and only if one of the linear factors is zero, each of the numbers  $s_1, s_2, \dots, s_k$  is a root of  $f(x)$  and there are no other roots.

$s_i$  is called a root of order  $m_i$ , or an  $m_i$ -fold root, or a root of multiplicity  $m_i$ .

If  $m_i = 1$ ,  $s_i$  is called a simple root; if  $m_i = 2$  it is a double root; if  $m_i = 3$ , a triple root; etc. A root which is not a simple root is called a multiple root. Although not every root need be a multiple root, every root has some multiplicity.

From the unique factorization into linear factors we see that if  $f(x)$  is of degree  $n \geq 1$  the sum of the multiplicities of its roots is  $n$ .

By "the roots" of  $f(x)$  we mean all the roots of  $f(x)$  each counted as often as its multiplicity. More precisely, we mean numbers  $r_1, r_2, \dots, r_n$  such that

$$\begin{aligned} r_i &= s_1 \text{ for exactly } m_1 \text{ values of } i \\ r_i &= s_2 \text{ for exactly } m_2 \text{ values of } i \\ &\vdots \\ r_i &= s_k \text{ for exactly } m_k \text{ values of } i \end{aligned}$$

Because of the unique factorization into linear factors, "the roots" of  $f(x)$  are unique. That is, if  $r_1, r_2, \dots, r_n$  are "the roots" and  $t_1, t_2, \dots, t_n$  are also "the roots," then the  $t$ 's can be renumbered, if necessary, so that  $r_1 = t_1, r_2 = t_2, \dots, r_n = t_n$ .

We can now state:

### THEOREM

*If  $f(x)$  is of degree  $n \geq 1$ , the roots of  $f(x)$  are  $n$  in number. They are the numbers  $r_1, r_2, \dots, r_n$  in the factorization  $f(x) \equiv a(x - r_1)(x - r_2) \cdots (x - r_n)$ .*

In order to determine the multiplicity of a root  $r$  of  $f(x)$ , it is not necessary to factor  $f(x)$  completely. It is necessary only to see "how many times"  $x - r$  is a factor. That is:

### THEOREM

*The multiplicity of a root  $r$  of  $f(x)$  is  $m$  if  $(x - r)^m$  is the highest power of  $x - r$  by which  $f(x)$  is divisible.*

*Proof:* Let  $f(x) \equiv (x - r)^m g(x)$ . Since  $f(x)$  is not divisible by  $(x - r)^{m+1}$ ,  $g(x)$  is not divisible by  $x - r$ .

Let the factorization of  $g(x)$  into linear factors be  $a(x - s_1)^{m_1} \cdots (x - s_k)^{m_k}$ . Then  $f(x) \equiv a(x - r)^m (x - s_1)^{m_1} \cdots (x - s_k)^{m_k}$ .

Since  $r, s_1, \dots, s_k$  are distinct,  $r$  is a root of  $f(x)$  of multiplicity  $m$ .

*Example* Determine the multiplicity of the root 2 of  $x^4 - 3x^3 + x^2 + 4$

Direct test shows that the polynomial is divisible by  $x - 2$  and by  $(x - 2)^2$  and not by  $(x - 2)^3$ . Thus, 2 is a double root.

**3. Synthetic division** Because of the frequency with which we have to divide a polynomial by one of the form  $x - r$  it would be convenient to be able to do so with a minimum of effort. The method of synthetic division, which we are about to describe, enables us to perform such a division quickly.

If  $f(x) \equiv a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ , then, by the division algorithm (§6, Ch. 2),  $f(x) \equiv (x - r)g(x) + c$ , where  $c$  is a constant.

If  $g(x) \equiv b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-2}x + b_{n-1}$ , then

$$\begin{aligned} a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ \equiv (x-r)(b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-2}x + b_{n-1}) + c \\ \equiv b_0x^n + (b_1 - rb_0)x^{n-1} + (b_2 - rb_1)x^{n-2} + \cdots \\ + (b_{n-1} - rb_{n-2})x + (c - rb_{n-1}) \end{aligned}$$

Equating coefficients, and transposing,

$$b_0 = a_0, \quad b_1 = a_1 + rb_0, \quad b_2 = a_2 + rb_1, \quad \cdots, \quad b_{n-1} = a_{n-1} + rb_{n-2}, \\ c = a_n + rb_{n-1}$$

This can be arranged conveniently as follows:

$$\begin{array}{cccccccc} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n & & |r \\ \hline & rb_0 & rb_1 & \cdots & rb_{n-2} & rb_{n-1} & & \\ b_0 & b_1 & b_2 & \cdots & b_{n-1} & c & & \end{array}$$

We first write on a horizontal line the coefficients of the powers of  $x$  in  $f(x)$ , arranged according to descending powers of  $x$  (Zero coefficients must be written down and not overlooked). Skipping a space, we draw a line. Below the line we write  $a_0$  (which is also  $b_0$ ) directly under the  $a_0$ . We multiply  $b_0$  by  $r$  and place  $rb_0$  on the second line underneath  $a_1$ . We add  $a_1$  and  $rb_0$  and write the result, which is  $b_1$ , directly underneath. We continue in the same way, multiplying  $b_1$  by  $r$  and placing the result  $rb_1$  on the second line directly underneath  $a_2$ . We add  $a_2$  and  $rb_1$  and write the result, which is  $b_2$ , directly underneath. Etc.

For example, to divide  $3x^3 - 2x^2 + 4$  by  $x + 2$  (here  $r = -2$ ),

$$\begin{array}{cccc} 3 & -2 & 0 & 4 & | -2 \\ & -6 & 16 & -32 & \\ \hline 3 & -8 & 16 & -28 & \end{array}$$

On the first line we have written the coefficients of  $f(x)$ . On the third line we write 3 directly under the 3 on the first line. Multiplying 3 by  $-2$ , we place  $-6$  on the second line below  $-2$ . Adding  $-2$  and  $-6$ , we place  $-8$  on the third line. We multiply  $-8$  by  $-2$  and place the 16 on the second line beneath the 0. Adding 0 and 16, we place the result on the third line. We multiply 16 by  $-2$ , place  $-32$  underneath the 4, and add.

The quotient and remainder are read from the third line, the last term being the remainder. Here the quotient is  $3x^2 - 8x + 16$  and the remainder is  $-28$ .



As another illustration we work the example of §2 by successive synthetic divisions. To determine the multiplicity of the root 2 of  $x^4 - 3x^3 + x^2 + 4$  we divide by  $x - 2$ ,

$$\begin{array}{r|rrrrr}
 1 & -3 & 1 & 0 & 4 & 2 \\
 & 2 & -2 & -2 & -4 & \\
 \hline
 1 & -1 & -1 & -2 & 0 & \\
 & 2 & 2 & 2 & & \\
 \hline
 1 & 1 & 1 & 0 & & \\
 & 2 & 6 & & & \\
 \hline
 1 & 3 & 7 & & & 
 \end{array}$$

Thus,  $f(x) \equiv (x - 2)(x^3 - x^2 - x - 2) \equiv (x - 2)^2(x^2 + x + 1)$ , and  $x^2 + x + 1$  is not divisible by  $x - 2$  since the remainder is 7.

The remaining roots of  $f(x)$  are the roots of  $x^2 + x + 1 = 0$ , i.e.,  $\frac{1}{2}(-1 \pm i\sqrt{3})$ . Thus the roots of  $f(x)$  are 2, 2,  $\frac{1}{2}(-1 + i\sqrt{3})$ ,  $\frac{1}{2}(-1 - i\sqrt{3})$ .

### Exercises

- Determine whether the given numbers are roots of the given polynomials and, if they are, find their multiplicities. If possible, factor into linear factors.
  - $2, x^4 - x^3 - 18x^2 + 52x - 40$
  - $2, 9x^4 - 12x^3 + 13x^2 - 12x + 4$
  - $-1/2, 8x^5 + 12x^4 + 11x^3 + 13x^2 + 6x + 1$
  - $2i, 9x^6 + 12x^5 + 40x^4 + 48x^3 + 52x^2 + 48x + 16$
  - $-i, 4x^7 + 4x^5 + 9x^4 + 8x^3 + 6x^2 + 4x + 1$
- Form an equation of which the roots are:
  - $0, 0, 2, 2, 2$
  - $1 + \sqrt{3}, 1 - \sqrt{3}, 1 - \sqrt{3}$
  - $i, i, 0, 1, 2i$
  - $-1/2, 1/2, 1, 0$
  - $1 - 3i, 1 - 3i, 1 + 3i, 1 + 3i$
- $ax^2 + bx + c = 0, a \neq 0$ , has a multiple root if and only if  $b^2 - 4ac = 0$ .
- 0 is a root of  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, a_0 \neq 0$ , of multiplicity  $k$  if and only if  $a_n = a_{n-1} = \cdots = a_{n-k+1} = 0, a_{n-k} \neq 0$ .
- A polynomial of degree  $n$  cannot have more than  $\frac{1}{2}n$  multiple roots.
- If  $r$  is a  $p$ -fold root of  $f(x)$  and a  $q$ -fold root of  $g(x)$ , it is a  $(p + q)$ -fold root of  $f(x)g(x)$ .
- $f(x) \not\equiv 0$  and  $g(x) \equiv 0$  have the same roots if and only if  $f(x) \equiv cg(x)$  where  $c$  is a constant.
- If  $f(x)$  and  $g(x)$  are factors of  $h(x)$  and have no common roots, then  $f(x)g(x)$  is a factor of  $h(x)$ .

- 9 If there is a number  $M$  such that  $|f(x)| \leq M$  for every  $x$ , then  $f(x)$  is a constant.
- 10 If every root of  $f(x) \equiv x^4 + ax^3 + bx^2 + cx + d$  is a multiple root, then there exists a polynomial  $g(x)$  such that  $f(x) \equiv g^2(x)$ .
- 11 If 1 is a root of  $2x^4 - 5x^3 + (2a + 3)x^2 - (a + 2)x + 1$ , show that it is a multiple root and find the roots.
- 12 Show that  $-2$  cannot be a multiple root of  $x^3 + x^2 - ax - 4 = 0$ .
- 13 For what values of  $a$  is  $a$  a root of  $2x^4 - 3ax^3 - a^2x^2 + 3a^2x - a^2 = 0$ ? What is its multiplicity?
- 14 If the  $n$ th power of every root of  $f(x)$  is a root, where  $n$  is an integer greater than 1, show that every root of  $f(x)$  is 0 or a root of unity.
- 15 Determine  $a$  and  $b$  so that  $-1$  shall be a multiple root of  $2x^6 + 8x^5 + 9x^4 - 4x^3 + ax^2 - 12x + b = 0$ .
- 16 Determine  $a$  and  $b$  so that 1 shall be a double root of  $x^4 + ax^3 + (a - b)x^2 + bx + 1 = 0$ .
- 17 Show that  $a$  is a multiple root of  $x^4 + 2ax^3 - 3a^2x^2 + (b + 2 - 4a^2)x + 4a^4 = 0$  if and only if  $b = -2$ .
- 18 If there is a number  $M$  such that  $|f(x)| \leq M|g(x)|$  for every  $x$ , then  $f(x) \equiv cg(x)$  where  $c$  is a constant. (Exercise 9 is a special case with  $g \equiv 1$ .)
- 19 From the fundamental theorem of algebra and the factor theorem (without using the unique factorization theorem of §12, Ch. 2), establish that every non-constant polynomial is uniquely factorable into linear factors.
- 20 Assuming that every non-constant polynomial with real coefficients has at least one complex root, prove that every non-constant polynomial with complex coefficients has at least one root. [Hint: If the coefficients of  $g(x)$  are the conjugates of those of  $f(x)$ , show that  $f(x)g(x)$  has real coefficients.]

#### A. Relations between roots and coefficients Let $n \geq 1$ ,

$$\begin{aligned} f(x) &\equiv x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ &\equiv (x - r_1)(x - r_2) \cdots (x - r_n) \end{aligned}$$

By multiplying the linear factors and comparing the resulting coefficients with  $a_1, a_2, \dots, a_n$ , we obtain relations among the roots and the coefficients of  $f(x)$ .

If  $n = 1$  then  $f(x) \equiv x + a_1$ , so that  $r_1 = -a_1$ .

If  $n = 2$  then  $f(x) \equiv x^2 + a_1x + a_2 \equiv (x - r_1)(x - r_2) \equiv x^2 - (r_1 + r_2)x + r_1r_2$ , so that  $r_1 + r_2 = -a_1, r_1r_2 = a_2$ .

If  $n = 3$  then

$$\begin{aligned} f(x) &\equiv x^3 + a_1x^2 + a_2x + a_3 \\ &\equiv (x - r_1)(x - r_2)(x - r_3) \\ &\equiv x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3 \end{aligned}$$

so that  $r_1 + r_2 + r_3 = -a_1$ ,  $r_1r_2 + r_1r_3 + r_2r_3 = a_2$ ,  $r_1r_2r_3 = -a_3$ .

To express the general result, denote by  $S_1$  the sum of all the roots taken singly, that is,  $r_1 + r_2 + \dots + r_n$ ,  $S_2$  the sum of all the products of the roots taken two at a time, that is,

$$r_1r_2 + r_1r_3 + \dots + r_1r_n + r_2r_3 + r_2r_4 + \dots + r_2r_n + \dots + r_{n-1}r_n,$$

$S_3$  the sum of all the products of the roots taken three at a time, that is,

$$r_1r_2r_3 + r_1r_2r_4 + \dots + r_2r_3r_4 + \dots + r_{n-2}r_{n-1}r_n$$

etc.

In general, let  $S_i$  be the sum of all possible products  $r_{j_1}r_{j_2}\dots r_{j_i}$ , where  $j_1, j_2, \dots, j_i$  are any  $i$  distinct numbers from  $1, 2, \dots, n$ . The greatest value that  $i$  can have is  $n$  and, in particular,  $S_n = r_1r_2\dots r_n$ .

#### THEOREM

$$S_1 = -a_1, S_2 = a_2, \dots, S_i = (-1)^i a_i, \dots, S_n = (-1)^n a_n.$$

*Proof:* We have already proved this for  $n = 1, 2, 3$ . Proceeding by mathematical induction, suppose it true for  $n = k$  and let  $n = k + 1$ .

If  $g(x) = (x - r_1)(x - r_2)\dots(x - r_k) = x^k + b_1x^{k-1} + \dots + b_k$ , then

$$\begin{aligned} x^{k+1} + a_1x^k + \dots + a_{k+1} &\equiv (x - r_1)(x - r_2)\dots(x - r_{k+1}) \\ &\equiv (x^k + b_1x^{k-1} + \dots + b_k)(x - r_{k+1}) \\ &\equiv x^{k+1} + (b_1 - r_{k+1})x^k \\ &\quad + (b_2 - r_{k+1}b_1)x^{k-1} + (b_3 - r_{k+1}b_2)x^{k-2} \\ &\quad + \dots + (b_k - r_{k+1}b_{k-1})x - r_{k+1}b_k \end{aligned}$$

Hence,  $a_1 = b_1 - r_{k+1}$ ,  $a_i = b_i - r_{k+1}b_{i-1}$  for  $i = 2, 3, \dots, k$ ,  $a_{k+1} = -r_{k+1}b_k$ .

By the hypothesis of the induction applied to  $g(x)$ ,  $b_i = (-1)^i S'_i$  ( $i = 1, 2, \dots, k$ ) where  $S'_i$  is the sum of the products of  $r_1, r_2, \dots, r_k$  taken  $i$  at a time

Therefore,

$$\begin{aligned} a_1 &= b_1 - r_{k+1} = -(r_1 + r_2 + \cdots + r_k) - r_{k+1} = -S_1 \\ a_{k+1} &= -r_{k+1}b_k = -r_{k+1}[(-1)^k r_1 r_2 \cdots r_k] = (-1)^{k+1} r_1 r_2 \cdots r_k r_{k+1} = (-1)^{k+1} S_{k+1} \\ a_i &= b_i - r_{k+1}b_{i-1} \quad (i = 2, 3, \dots, k) \\ &= (-1)^i S'_i - r_{k+1}(-1)^{i-1} S'_{i-1} = (-1)^i (S'_i + r_{k+1} S'_{i-1}) \end{aligned}$$

$S'_{i-1}$  contains all the products of  $r_1, r_2, \dots, r_k$  taken  $i-1$  at a time. Therefore  $r_{k+1}S'_{i-1}$  contains all those products of  $r_1, r_2, \dots, r_k, r_{k+1}$  taken  $i$  at a time which have  $r_{k+1}$  as a factor. All the products of  $r_1, r_2, \dots, r_k, r_{k+1}$  taken  $i$  at a time which do not have  $r_{k+1}$  as a factor are in  $S'_i$ . Thus  $S'_i + r_{k+1}S'_{i-1}$  is the sum of all the products of  $r_1, r_2, \dots, r_k, r_{k+1}$  taken  $i$  at a time. Hence  $S'_i + r_{k+1}S'_{i-1} = S_i$ , which proves the theorem for  $n = k+1$ .

By the principle of mathematical induction, the theorem is completely proved.

*Remark* The theorem states that the roots of  $f(x)$  satisfy the  $n$  equations  $S'_i = (-1)^i a_i$  ( $i = 1, 2, \dots, n$ ). Conversely, if  $r_1, r_2, \dots, r_n$  are numbers satisfying these equations, then they are the roots of  $f(x)$ . For if  $g(x) \equiv (x - r_1)(x - r_2) \cdots (x - r_n) \equiv x^n + b_1 x^{n-1} + \cdots + b_{n-1} x + b_n$ , then by the theorem  $b_i = (-1)^i S'_i$  for  $i = 1, 2, \dots, n$ . By hypothesis  $S'_i = (-1)^i a_i$ . Therefore  $b_i = (-1)^i (-1)^i a_i = (-1)^{2i} a_i = a_i$ . Thus  $g(x) \equiv f(x)$ , so that  $r_1, r_2, \dots, r_n$  are the roots of  $f(x)$ .

*Example 1* If  $r, s, t$  are the roots of  $x^3 - ax^2 + bx + c = 0$ , evaluate  $r^2 + s^2 + t^2$ . We have  $r^2 + s^2 + t^2 = (r + s + t)^2 - 2(rs + rt + st) = a^2 - 2b$ .

*Example 2* Determine  $a$  so that one root of  $x^3 - ax^2 + ax - 4 = 0$  shall be the reciprocal of another, and find the roots.

Let the roots be  $r, 1/r, s$ . By the relations among the roots and coefficients,

$$\begin{aligned} r + \frac{1}{r} + s &= a \\ r \frac{1}{r} + rs + \frac{1}{r} s &= a \\ r \frac{1}{r} s &= 4 \end{aligned}$$

From the last equation,  $s = 4$ . The first two become

$$r + \frac{1}{r} + 4 = a$$

$$1 + 4\left(r + \frac{1}{r}\right) = a$$

Solving the first of these for  $r + \frac{1}{r}$  and substituting into the second, gives  $1 + 4(a - 4) = a$ , from which  $a = 5$ .

Thus, if one root is the reciprocal of another, then  $a = 5$ . Conversely, suppose  $a = 5$ . Then the three equations above are

$$r + \frac{1}{r} + s = 5$$

$$1 + rs + \frac{s}{r} = 5$$

$$s = 4$$

If there exist values of  $r$  and  $s$  satisfying all three of these, then, by the Remark above,  $r, 1/r, s$  are the roots of the polynomial with  $a = 5$ . We leave it to the reader to verify that  $s = 4, r = \frac{1}{2}(1 \pm i\sqrt{3})$  are the solutions of these equations. (Note that each of the values of  $r$  is the reciprocal of the other.) Hence the roots are 4,  $\frac{1}{2}(1 + i\sqrt{3}), \frac{1}{2}(1 - i\sqrt{3})$ .

### Exercises

1 Determine the roots and the unknown coefficients under the given conditions

- One root of  $x^3 - 2x^2 + ax - 1 = 0$  is the negative of another.
- One root of  $2x^4 - 11x^3 + a - 0$  is double another.
- The roots of  $x^3 + 3x^2 + 4x + a = 0$  are in arithmetic progression.
- The roots of  $5x^4 - 63x^3 + 21x + a = 0$  are in geometric progression.
- The roots of  $x^3 + 6x^2 + ax + b = 0$  are in the ratios 1:2:3.
- One root of  $x^3 + 8x^2 - 21x + a = 0$  is three times another.
- $x^4 - 4x^3 + ax^2 + 4x + b = 0$  has two pairs of equal roots.
- $x^4 - 4x^3 + 6x^2 + ax + b = 0$  has two pairs of roots with one root in each pair equal to the other in the pair increased by 2.
- One root of  $x^4 + 2x^3 + ax - 1 = 0$  is the reciprocal of another.
- Every root of  $x^4 + 4x^3 + 4x^2 + ax^2 + bx + c = 0$  is a multiple root.
- $x^4 - 3ax^3 + 18x^2 - 12ax + b = 0$  has two pairs of roots with one root in each pair the double of the other in the pair.
- The reciprocal of every root of  $x^3 + ax^2 + bx - 2 = 0$  is a root.

- m) Whenever  $r$  is a root of  $x^3 + 3x^2 + ax + b = 0$ ,  $(r + 3)/(r - 1)$  is a root.
- n) Every root of  $x^3 + ax^2 + ax + a = 0$  is an integer.
- o) The product of any two of the roots of  $x^3 + ax^2 + bx + c = 0$  equals the third.
- 2 If  $r, s, t$  are the roots of  $x^3 + ax^2 + bx + c = 0$ , evaluate
- $r^3st + s^3rt + t^3rs$
  - $\frac{1}{r} + \frac{1}{s} + \frac{1}{t}$  if  $c \neq 0$
  - $(r - 1)(s - 1)(t - 1)$
  - $rs^2 + rt^2 + r^2s + st^2 + r^2t + s^2t$
  - $\frac{r+s}{t} + \frac{r+t}{s} + \frac{s+t}{r}$  if  $c \neq 0$
  - $\frac{1}{r^2} + \frac{1}{s^2} + \frac{1}{t^2}$  if  $c \neq 0$
  - $r(s+1)^2 + r(t+1)^2 + s(r+1)^2 + s(t+1)^2 + t(r+1)^2 + t(s+1)^2$
  - $r^3 + s^3 + t^3$
- 3 If  $r, s, t$  are the roots of  $x^3 + ax^2 + bx + c = 0$ , then:
- One root is the negative of another if and only if  $ab = c$ .
  - One root is the reciprocal of another if and only if  $c(a - c) = b - 1$ .
  - The sum of two of the roots is 1 if and only if  $c = (a + 1)(a + b + 1)$ .
  - The negative of every root is a root if and only if  $a = c = 0$  or  $b = -a^2, c = -a^3$ .
  - $1/r, 1/s, 1/t$ , when  $c \neq 0$ , are the roots if and only if  $c = 1, a = b$  or  $c = -1, a = -b$ .
  - $r, s, t$ , taken in some order, are in geometric progression if and only if  $b^2 = a^2c$ .
  - If  $a = 0$ , there is a multiple root if and only if  $4b^3 + 27c^2 = 0$ .
- 4 Show that  $x^4 + ax^3 + bx^2 + cx + d = 0$  has two pairs of roots such that in each pair,
- One root is the negative of the other if and only if  $a = c = 0$ .
  - One root is the reciprocal of the other if and only if  $d = 1, a = c$ .
- 5 The sum of the squares of the roots of  $x^n + a_1x^{n-1} + \dots + a_n = 0$ ,  $n \geq 2$ , equals the square of their sum if and only if  $a_2 = 0$ .
- 6 If  $a$  is positive, at least one root of  $x^4 + ax^2 + bx + c = 0$  is imaginary.
- 7 If  $n \geq 2$ , under what conditions on  $a, b, n$  will all the roots of  $x^n - nx^{n-1} + b = 0$  be equal?
- 8 If  $r_1, r_2, r_3$  are the roots of  $x^3 - 3x + 3 = 0$  and  $s_1, s_2, s_3$  the roots of  $x^3 - x^2 - 1 = 0$ , find the sum of the nine numbers  $(r_i + s_j)^2$ .

**5. Transformations of the roots** The problem sometimes arises of finding a polynomial whose roots bear a specified relationship to

the roots of a given polynomial  $f(x)$  without first finding the roots of  $f(x)$ . For instance, suppose we seek a polynomial whose roots are  $2/r$ ,  $2/s$ ,  $2/t$ , where  $r$ ,  $s$ ,  $t$  are the roots of  $f(x) \equiv x^3 + ax^2 + bx + c = 0$ ,  $c \neq 0$ .

*First solution* From the relations among the roots and coefficients, we have

$$\begin{aligned}\frac{2}{r} + \frac{2}{s} + \frac{2}{t} &= 2 \frac{st + rt + rs}{rst} = \frac{2b}{-c} \\ \frac{2}{r} \frac{2}{s} + \frac{2}{r} \frac{2}{t} + \frac{2}{s} \frac{2}{t} &= 4 \frac{t + s + r}{rst} = 4 \frac{-a}{-c} \\ \frac{2}{r} \frac{2}{s} \frac{2}{t} &= \frac{8}{rst} = \frac{8}{-c}\end{aligned}$$

Therefore, one polynomial with the desired roots is  $x^3 + (2b/c)x^2 + (4a/c)x + 8/c$ . Multiplying by  $c$ , we obtain another,  $cx^3 + 2bx^2 + 4ax + 8$ .

*Second solution* Let  $y = 2/x$ . Then  $x = 2/y$ . In  $f(x) = 0$  replace  $x$  by  $2/y$  and multiply through by  $y^3$ . We obtain  $cy^3 + 2by^2 + 4ay + 8 = 0$ .

To justify this method, denote the polynomial in  $y$  by  $g(y)$ . Then, from the way in which it was obtained,  $g(y) = y^3 f(2/y)$  for  $y \neq 0$ .

Since  $f(x) \equiv (x - r)(x - s)(x - t)$ , therefore for  $y \neq 0$

$$\begin{aligned}g(y) &= y^3 \left( \frac{2}{y} - r \right) \left( \frac{2}{y} - s \right) \left( \frac{2}{y} - t \right) = (2 - ry)(2 - sy)(2 - ty) \\ &= -rst \left( y - \frac{2}{r} \right) \left( y - \frac{2}{s} \right) \left( y - \frac{2}{t} \right) \\ &= c \left( y - \frac{2}{r} \right) \left( y - \frac{2}{s} \right) \left( y - \frac{2}{t} \right)\end{aligned}$$

The last expression is a polynomial in  $y$ . So is  $g(y)$ . Since they are equal for all values of  $y$  except possibly  $y = 0$ , they are equal for infinitely many values of  $y$ . Hence they are identical (§4, Ch. 2).

From the factored form for  $g(y)$ , we see that  $2/r$ ,  $2/s$ ,  $2/t$  are the roots of  $g(y)$ .

### Exercises

- 1 If  $r$ ,  $s$ ,  $t$  are the roots of  $x^3 + ax^2 + bx + c = 0$ , find an equation for which the roots are:

- a)  $3r, 3s, 3t$
  - b)  $-r, -s, -t$
  - c)  $rs, rt, st$
  - d)  $r^2, s^2, t^2$
  - e)  $1/rs, 1/rt, 1/st$  if  $c \neq 0$
  - f)  $r + 2, s + 2, t + 2$
  - g)  $(2/r) - 2, (2/s) - 2, (2/t) - 2$  if  $c \neq 0$
  - h)  $(r-1)/(r+1), (s-1)/(s+1), (t-1)/(t+1)$  if  $r \neq -1, s \neq -1, t \neq -1$
  - i)  $rs/t, rt/s, st/r$  if  $c \neq 0$
  - j)  $r + s, r + t, s + t$
  - k)  $r + s - t, r + t - s, s + t - r$
  - l)  $\sqrt{r}, -\sqrt{r}, \sqrt{s}, -\sqrt{s}, \sqrt{t}, -\sqrt{t}$  where  $\sqrt{r}, \sqrt{s}, \sqrt{t}$  are any square roots of  $r, s, t$
- 2 Prove. The roots of  $a_0x^n - a_1x^{n-1} + a_2x^{n-2} - a_3x^{n-3} + \cdots + (-1)^na_n$  are the negatives of the roots of  $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ . Hence, find a polynomial whose roots are the negatives of the roots of:
- a)  $x^3 - 3x^2 - 3x + 5 = 0$
  - b)  $3x^3 + x^2 - 7x + 4 = 0$
  - c)  $4x^6 + 2x^5 - x^2 + x - 1 = 0$
  - d)  $2x^4 + 2x^3 - 3x^2 + 4x = 0$
  - e)  $3x^3 - 3x^2 - 2 = 0$
- 3 Prove: If  $a_0 \neq 0, a_n \neq 0$ , the roots of  $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$  are the reciprocals of the roots of  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ . Hence, find equations whose roots are the reciprocals of the roots of the equations in ex. 2
- 4 Prove: The roots of  $a_0x^n + a_1kx^{n-1} + a_2k^2x^{n-2} + \cdots + a_{n-1}k^{n-1}x + a_nk^n = 0$  are the roots of  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$  each multiplied by  $k$ . Hence, find equations whose roots are the roots of the equations in ex. 2 each multiplied by (a)  $-2$ , (b)  $1/3$ , (c)  $i$ .
- 5 For each of the equations in ex. 2 find a  $k$  so that an equation whose roots are the roots of these equations multiplied by  $k$  shall have integral coefficients and leading coefficient 1.
- 6 Show, by the second transformation method above, how to find a polynomial whose roots are those of  $f(x)$  each increased by  $h$ .
- 7 If  $r_1, r_2, \dots, r_n$  are the roots of  $f(x) = 0$ , and  $\alpha, \beta, \gamma, \delta$  are constants, not both  $\alpha$  and  $\gamma$  zero, and none of the numbers  $\gamma r_i + \delta$  ( $i = 1, 2, \dots, n$ ) is zero, show that the second method above is applicable to finding an equation for which the roots are  $(\alpha r_i + \beta)/(\gamma r_i + \delta)$  ( $i = 1, 2, \dots, n$ ).
- 8 Find an equation the roots of which all differ from the roots of  $x^3 + ax^2 + bx + c = 0$  by the same number and in which the coefficient of  $x^2$  is zero.



- 9 Let  $f(x) \equiv f_1(x) + f_2(x)$  where  $f_1(x)$  contains the terms of  $f(x)$  involving odd powers of  $x$  and  $f_2(x)$  those involving even powers. Write  $f(x) = 0$  in the form  $f_1(x) = -f_2(x)$  and square both sides. Show that in the resulting equation only even powers of  $x$  appear. In this equation replace  $x^2$  by  $y$ . Show that the roots of the equation in  $y$  are the squares of the roots of  $f(x) = 0$ . [Hint: Show  $f_2^2(x) - f_1^2(x) \equiv f(x)f(-x)$ .]

**6. Common roots** To find the common roots of two polynomials it is usually not necessary to find all the roots of either one, as the following theorem shows.

### THEOREM

*If  $D(x)$  is a H.C.F. of  $f(x)$  and  $g(x)$ ,  $r$  is a common root of  $f(x)$  and  $g(x)$  if and only if  $r$  is a root of  $D(x)$ .*

*Proof:* By the factor theorem (§3, Ch. 2), if  $r$  is a common root of  $f(x)$  and  $g(x)$ ,  $x - r$  is a common factor. But every common factor is a factor of  $D(x)$ , by definition of a H.C.F. (§8, Ch. 2). Hence, if  $r$  is a common root of  $f(x)$  and  $g(x)$  it is a root of  $D(x)$ .

Conversely, if  $r$  is a root of  $D(x)$ ,  $x - r$  is a factor of  $D(x)$  and, therefore, also of  $f(x)$  and of  $g(x)$ . Hence, it is a common root.

*Example 1* Find the common roots, if any, of  $x^4 - x^3 + 3x^2 - 2x + 2$  and  $x^3 - 2x^2 + 2x - 4$ .

By the Euclidean algorithm,  $x^2 + 2$  is a H.C.F. Hence, the common roots are  $\pm i\sqrt{2}$ .

*Example 2* Show, without finding all the roots, that the negative reciprocal of one of the roots of  $f(x) \equiv x^4 + (1 + i)x + 1$  is a root.

We first find a polynomial whose roots are the negative reciprocals of the roots of  $f(x)$ . Using the second method of §5, we let

$y = \frac{-1}{x}$  and obtain  $g(y) \equiv y^4 - (1 + i)y^2 - 1$ .

If  $r, s, t$  are the roots of  $f(x)$ , the roots of  $g(y)$  are  $-\frac{1}{r}, -\frac{1}{s}, -\frac{1}{t}$ .

Thus, one of  $-\frac{1}{r}, -\frac{1}{s}, -\frac{1}{t}$  is a root of  $f(x)$  if and only if  $f(x)$  and  $g(y)$  have a common root. Further, every common root is a root of  $f(x)$  whose negative reciprocal is a root.

By the Euclidean algorithm we find that  $x - i$  is a H.C.F. of

$f(x)$  and  $g(x)$ . Thus,  $i$  is a root of  $f(x)$  whose negative reciprocal  $-\frac{1}{i} = i$  is a root.

### Exercises

- 1 Prove: A common root of  $f(x)$  and  $g(x)$  is a root of every remainder in the Euclidean algorithm. (Thus, when we arrive at a remainder whose roots can be found easily we can determine the common roots without carrying the algorithm to its conclusion.)
- 2 Find the common roots, if any, of the pairs of polynomials in ex. 4, §9, Ch. 2.
- 3 Show, without finding all the roots, that one root of
  - a)  $4x^4 + 4x^3 - 5x^2 - 9x - 9 = 0$  is the negative of another
  - b)  $2x^4 - x^3 + 5x^2 - x + 3 = 0$  is the reciprocal of another
  - c)  $18x^3 + 9x^2 - 5x - 2 = 0$  is twice another
  - d)  $4x^3 - 13x + 6 = 0$  differs from another by 1
  - e)  $2x^3 - x^2 - x - 3 = 0$  is the square of another
- 4 Find the values of  $k$  for which there is a common root:
  - a)  $x^5 - 2x^3 - 3x^2 + 4 = 0$ ,  $x^4 + x^3 - x^2 - kx - k = 0$
  - b)  $x^3 - 2x^2 + k = 0$ ,  $x^3 - 3x + 2k = 0$
  - c)  $x^3 - 2x + k - 1 = 0$ ,  $x^4 - 2x^2 - kx + 2k - 1 = 0$
  - d)  $x^3 - 6x^2 + 3x - 2k = 0$ ,  $x^5 - 15x - 14k = 0$
  - e)  $x^4 + kx^3 + k^2 - 1 = 0$ ,  $x^4 + kx - 1 = 0$
  - f)  $x^3 - (k^2 + 1)x + k = 0$ ,  $x^3 - (k + 1)x^2 + k^2 = 0$
  - g)  $x^3 + (3k - 2)x^2 + (3k^2 - 4k)x + k^2(k - 2) = 0$ ,  $x^3 + (3k - 1)x^2 + (3k^2 - 2k - 1)x + (k^2 - 1)(k - 1) = 0$
- 5 Show that there is no common root if  $k$  is real:
  - a)  $x^3 + x^2 + (k - 1)x + k - 2 = 0$ ,  $x^2 + x + k = 0$
  - b)  $x^3 - kx^2 - kx - k - 1 = 0$ ,  $x^3 - kx^2 + kx - k + 1 = 0$
- 6 For what values of  $a$  and  $b$  is there a common root?
  - a)  $x^3 + ax + b = 0$ ,  $x^n + x^3 + ax + b = 0$ ,  $n > 3$
  - b)  $x^3 + ax^2 + b = 0$ ,  $x^4 + (a + 1)x^3 + (a + 1)x^2 + bx + b = 0$
  - c)  $x^3 + (a + 1)x^2 + (a + 1 - b^2 + ab)x + ab - b^2 + b = 0$ ,  $x^3 + ax^2 + (1 - b^2 + ab)x + b = 0$
- 7 If  $a \neq 0$  and  $x^3 - 3a^2x + b = 0$  and  $x^3 - 2a^2x + b - a^3 = 0$  have a common root, then the first equation has a multiple root.
- 8  $f(x)$  and  $g(x)$  have a common root if and only if they are not relatively prime.
- 9 If  $f(x)$  and  $g(x)$  are in  $\mathbb{F}[x]$  and  $f(x)$  is irreducible over  $\mathbb{F}$ , and  $f(x)$  and  $g(x)$  have a common root, then  $f(x)$  is a factor of  $g(x)$ .
- 10 If  $f(x)$  and  $g(x)$  are in  $\mathbb{F}[x]$  and have exactly one common root, regardless of its multiplicity for either  $f(x)$  or  $g(x)$ , then that root is in  $\mathbb{F}$ .

- 11 If  $f(x)$  and  $g(x)$  are in  $\mathfrak{F}[x]$  and  $f(x)$  is irreducible over  $\mathfrak{F}$ , and every root of each is a root of the other, then  $g(x) \equiv cf^m(x)$ , where  $m$  is a positive integer and  $c$  is in  $\mathfrak{F}$ .
- 12 If  $f(x)$  is irreducible over  $\mathfrak{F}$ , it cannot have two distinct roots whose difference is in  $\mathfrak{F}$ .
- 13 If  $f(x)$  is a cubic polynomial in  $\mathfrak{F}[x]$  and has a non-zero root which is twice another root, then all the roots of  $f(x)$  are in  $\mathfrak{F}$ .

## DERIVATIVES AND MULTIPLE ROOTS

**1. Derivatives** When the values of  $x$  and  $f(x)$  are real numbers, the derivative of  $f(x)$  for any value of  $x$  is defined in the calculus as a certain limit. To extend this idea when  $x$  and  $f(x)$  have imaginary values first requires the extension of the concept of limit. For polynomials, however, we can avoid this by defining the derivative in a purely algebraic way.

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_{n-1} x + a_n$ , where the coefficients may be any complex numbers.

If  $n > 0$  we define the derivative of  $f(x)$  to be  $na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1$ .

If  $n = 0$  we define the derivative of  $f(x)$  to be the zero polynomial.

We denote the derivative of  $f(x)$  by  $f'(x)$ .

If  $f(x)$  is of degree  $n \geq 1$ ,  $f'(x)$  is of degree  $n - 1$  and if  $f(x)$  is a constant its derivative is zero.

The derivative of  $f'(x)$  is called the second derivative of  $f(x)$  and is denoted by  $f''(x)$ . The derivative of  $f''(x)$  is called the third derivative of  $f(x)$  and is denoted by  $f'''(x)$ . Etc.

The  $k$ th derivative  $f^{(k)}(x)$  is also called the derivative of order  $k$ .

It is sometimes convenient to refer to  $f(x)$  itself as its 0th derivative and to denote it by  $f^{(0)}(x)$ .

To differentiate a polynomial is to obtain its derivative. To differentiate it  $k$  times is to obtain its  $k$ th derivative.

From the purely algebraic definition we can obtain the usual rules for operating with derivatives.

## THEOREM

*The derivative of  $f(x) \pm g(x)$  is  $f'(x) \pm g'(x)$ .*

The proof is immediate.

## COROLLARY

*The derivative of a sum of polynomials is the sum of their derivatives.*

## THEOREM

*The derivative of  $f(x)g(x)$  is  $f(x)g'(x) + f'(x)g(x)$ .*

*Proof:* If either  $f(x) = 0$  or  $g(x) = 0$ , the desired result is immediate. Hence, suppose neither vanishes identically. Let the degree of  $f(x)g(x)$  be  $n$ .

If  $n = 0$  then  $f(x)$  and  $g(x)$  are constants and again the desired result is obvious.

Proceeding by mathematical induction, suppose the desired result established for  $n = 0, 1, \dots, k$ . Let  $n = k + 1$  and

$$f(x) = ax^p + f_1(x), \quad a \neq 0, \quad f_1(x) = 0 \text{ or of degree at most } p-1 \\ g(x) = bx^q + g_1(x), \quad b \neq 0, \quad g_1(x) = 0 \text{ or of degree at most } q-1$$

Then

$$f(x)g(x) = abx^{p+q} + ax^p g_1(x) + bx^q f_1(x) + f_1(x)g_1(x)$$

By the theorem above,

$$[f(x)g(x)]' = [abx^{p+q}]' + [(ax^p)g_1(x)]' + [(bx^q)f_1(x)]' + [f_1(x)g_1(x)]'$$

Each of the last three terms either vanishes identically or else the hypothesis of the induction applies to it. In either case

$$\begin{aligned} [f(x)g(x)]' &= (p+q)abx^{p+q-1} + ax^p g_1'(x) + pax^{p-1}g_1(x) \\ &\quad + bx^q f_1'(x) + qbx^{q-1}f_1(x) + f_1(x)g_1'(x) + f_1'(x)g_1(x) \\ &= [ax^p + f_1(x)][qbx^{q-1} + g_1'(x)] \\ &\quad + [pax^{p-1} + f_1'(x)][bx^q + g_1(x)] \\ &= f(x)g'(x) + f'(x)g(x) \end{aligned}$$

Thus, the desired result is established for  $n = k + 1$ .

By the principle of mathematical induction, the theorem is proved.

## Exercises

- 1 If  $f'(x) = 0$ ,  $f(x)$  is a constant.
- 2 If  $f'(x) = f'(c)$ , then  $f(x) = g(x) + c$  where  $c$  is a constant.
- 3 If  $f(x)$  is of degree  $n \geq 1$ , then  $f^{(k)}(x)$  is of degree  $n - k$  ( $k = 1, 2, \dots, n$ ). In particular,  $f^{(n)}(x) = n!a$  where  $a$  is the leading coefficient in  $f(x)$ .
- 4 If  $f^{(k)}(x) \equiv 0$ , then  $f(x)$  is identically zero or of degree less than  $k$ . (Exercise 1 is a special case with  $k = 1$ ).

- \*5 If  $m$  is a positive integer, the derivative of  $f^m(x)$  is  $mf^{m-1}(x)f'(x)$ . In particular, the derivative of  $(x-a)^m$  is  $m(x-a)^{m-1}$ .
- 6 The derivative of  $f(g(x))$  is  $f'(g(x))g'(x)$ . (This is called the composite function, or function of a function, formula.)
- 7 If the coefficients of  $f(x)$  are in field  $\mathfrak{F}$ , the coefficients of all the derivatives of  $f(x)$  are in  $\mathfrak{F}$ .
- 8 If  $g(x)$  and  $h(x)$  are relatively prime, neither a constant, and  $f(x) \equiv g(x)h(x)$ ,  $f'(x)$  is not divisible by  $g(x)$  or  $h(x)$ .
- 9 If  $c_0, c_1, \dots, c_k$  are constants,  $c_0 \neq 0$ , and  $c_0f(x) + c_1f'(x) + \dots + c_kf^{(k)}(x) \equiv 0$ , then  $f(x) \equiv 0$ .
- 10 If  $f(x) \equiv g(x)h(x)$ , then  $g(x)f'(x) - f(x)g'(x) \equiv g^2(x)h'(x)$ .
- 11 If  $g(x)f'(x) - f(x)g'(x)$  is divisible by  $g^2(x)$ , then  $f(x)$  is divisible by  $g(x)$ . (Hint: Let  $D$  be a H.C.F. of  $f$  and  $g$ ,  $f \equiv DF$ ,  $g \equiv DG$ .)
- 12 If  $f(x)g'(x) - g(x)f'(x) \equiv 0$ , then there exist constants  $a$  and  $b$ , not both zero, such that  $af(x) + bg(x) \equiv 0$ , and conversely. (Hint: Use ex. 11.)
- 13 If  $f(x) \equiv g(x)h(x)$ ,  $g(a) = 0$ ,  $g'(a) \neq 0$ , then  $h(a) = f'(a)/g'(a)$ . (This is a special case of l'Hospital's rule.)
- 14 Find all polynomials  $f(x)$  such that:
- $f''(x) \equiv 0$
  - $xf'(x) - 2f(x) \equiv x - 2$
  - $f''(x) - xf'(x) + 2f(x) \equiv 0$
  - $(x^2 + 1)f''(x) - 2xf'(x) + 2f(x) \equiv 0$
  - $x(x-1)f''(x) - (2x-1)f'(x) + 2f(x) \equiv 2x^4 - 3x^2$
- 15 Under what conditions will  $[f(x)g(x)]' = f'(x)g'(x)$ ?

## 2. Multiple roots

### THEOREM 1

If  $r$  is a root of  $f(x) \neq 0$ , its multiplicity is the smallest value of  $i$  for which  $f^{(i)}(r) \neq 0$ .

*Proof:* If the multiplicity of  $r$  is  $m$ , then  $f(x) \equiv (x-r)^mg(x)$  where  $g(r) \neq 0$  (§2, Ch. 3).

By the rules for differentiation (§1 and ex. 5, §1),

$$f'(x) \equiv (x-r)^mg'(x) + m(x-r)^{m-1}g(x) \equiv (x-r)^{m-1}g_1(x)$$

where  $g_1(r) = mg(r) \neq 0$ .

Differentiating again, we obtain in the same way

$$f''(x) \equiv (x-r)^{m-2}g_2(x)$$

where  $g_2(r) \neq 0$ .

Continuing in this way, we finally obtain

$$f^{(m-1)}(x) \equiv (x - r)g_{m-1}(x)$$

where  $g_{m-1}(r) \neq 0$ .

Differentiating once more,

$$f^{(m)}(x) = g_{m-1}(x) + (x - r)g'_{m-1}(x)$$

from which  $f^{(m)}(r) = g_{m-1}(r) \neq 0$ .

Hence,  $f^{(i)}(r) = 0$  for  $i = 1, 2, \dots, m - 1$  and  $f^{(m)}(r) \neq 0$ , and the theorem is proved.

#### THEOREM 2

*$r$  is a multiple root of  $f(x) \neq 0$  if and only if it is a common root of  $f(x)$  and  $f'(x)$ .*

*Proof:* Apply theorem 1.

#### THEOREM 3

*$r$  is a multiple root of  $f(x)$  if and only if it is a root of a H.C.F. of  $f(x)$  and  $f'(x)$ .*

*Proof:* Apply theorem 2 and the theorem of §6, Ch. 3.

#### THEOREM 4

*If  $r$  is a root of  $f(x)$  of multiplicity  $m$ , it is a root of  $f'(x)$  of multiplicity  $m - 1$  (where to take care of the case  $m = 1$ , a root of multiplicity zero is understood not to be a root).*

*Proof:* Apply theorem 1 to  $f'(x)$ .

#### THEOREM 5

*If  $r$  is a root of  $f(x)$  of multiplicity  $m$ , and  $D(x)$  is a H.C.F. of  $f(x)$  and  $f'(x)$ , then  $r$  is a root of  $D(x)$  of multiplicity  $m - 1$ .*

*Proof:* Let  $f(x) \equiv (x - r)^m g(x)$  where  $g(x)$  is not divisible by  $x - r$  (§2, Ch. 3).

By theorem 4,  $f'(x) \equiv (x - r)^{m-1} h(x)$  where  $h(x)$  is not divisible by  $x - r$ .

Since  $(x - r)^{m-1}$  is a factor of both  $f(x)$  and  $f'(x)$ , it is a factor of  $D(x)$ . Hence  $r$  is a root of  $D(x)$  of multiplicity  $m - 1$  or higher.

If  $r$  were a root of  $D(x)$  of multiplicity  $m$  or higher,  $D(x)$  would be divisible by  $(x - r)^m$ . Since  $D(x)$  is a factor of  $f'(x)$ ,  $f'(x)$  would also be divisible by  $(x - r)^m$ , which is impossible.

Thus,  $r$  is a root of  $D(x)$  of multiplicity  $m - 1$ , and the theorem is proved.

### THEOREM 6

If  $f(x)$  is of degree  $n \geq 1$ ,  $D(x)$  a H.C.F. of  $f(x)$  and  $f'(x)$ ,  $f(x) \equiv D(x)g(x)$ , then  $g(x) \equiv c(x - r_1)(x - r_2) \cdots (x - r_k)$  where  $c$  is a constant and  $r_1, r_2, \dots, r_k$  are the distinct roots of  $f(x)$ .

In other words,  $g(x)$  has the same roots as  $f(x)$ , but each root is simple.

*Proof:* Let  $f(x) \equiv a(x - r_1)^{m_1}(x - r_2)^{m_2} \cdots (x - r_k)^{m_k}$ , where  $r_1, r_2, \dots, r_k$  are the distinct roots of  $f(x)$  of multiplicities  $m_1, m_2, \dots, m_k$ .

By theorem 5, each  $r_i$  is a root of  $D(x)$  of multiplicity  $m_i - 1$ . Hence  $D(x) \equiv (x - r_1)^{m_1-1}(x - r_2)^{m_2-1} \cdots (x - r_k)^{m_k-1}h(x)$ , and none of the  $r_i$  is a root of  $h(x)$ .

Every root of  $h(x)$  is a root of  $f(x)$ , since  $D(x)$  is a factor of  $f(x)$ . Since none of the  $r_i$  is a root of  $h(x)$ , and  $f(x)$  has no roots besides these,  $h(x)$  has no roots. Therefore,  $h(x)$  is a non-zero constant, so that  $D(x) = b(x - r_1)^{m_1-1}(x - r_2)^{m_2-1} \cdots (x - r_k)^{m_k-1}$ .

Thus, if  $f(x) = D(x)g(x)$  then  $g(x) = (a/b)(x - r_1)(x - r_2) \cdots (x - r_k)$ , and the theorem is proved.

*Example* Test  $f(x) = x^6 + x^4 + 3x^2 + 2x + 2$  for multiple roots.

$$f'(x) = 6x^5 + 4x^3 + 6x + 2 = 2(3x^5 + 2x^3 + 3x + 1)$$

By the Euclidean algorithm,  $x^2 + x + 1$  is a H.C.F. of  $f(x)$  and  $f'(x)$ . The roots of this H.C.F. are  $\frac{1}{2}(-1 \pm i\sqrt{3})$ , each simple. Hence, each of these is a double root of  $f(x)$ .

Since  $\frac{1}{2}(-1 \pm i\sqrt{3})$  are double roots of  $f(x)$ ,  $[x - (-1 + i\sqrt{3})/2][x - (-1 - i\sqrt{3})/2] = (x^2 + x + 1)^2 = x^4 + 2x^3 + 3x^2 + 2x + 1$  is a factor. The other factor is  $x^2 - 2x + 2$ , with  $1 + i$  and  $1 - i$  as roots; these are the remaining two roots of  $f(x)$ .

### Exercises

1 Test for multiple roots:

- $x^6 + 80x^4 + 240x^2 + 192 = 0$
- $x^6 - 12x + 5 = 0$
- $x^6 - 6x^5 + 15x^4 - 20x^3 + 12x^2 - 4 = 0$
- $x^4 - 9x^3 + 23x^2 - 3x - 36 = 0$
- $x^4 - 9x^2 + 4x + 12 = 0$
- $x^3 - 6ix - 4i + 4 = 0$



- g)  $27x^6 + 45x^2 - 36x + 20 = 0$   
 h)  $x^5 - 5x^3 + 10x + 4 = 0$   
 i)  $x^6 - 9x^4 + 16x^2 - 9x^2 + 1 = 0$
- 2 Find all the values of  $k$ , if any, for which there is a multiple root:
- a)  $x^3 + 3kx + 16 = 0$   
 b)  $x^3 + 3kx^2 + 6kx + 4k = 0$   
 c)  $x^4 + 2x^2 + 4kx + 9k^2 + 1 = 0$   
 d)  $x^3 - 3kx + k = 0$   
 e)  $x^4 + 4kx + 3k = 0$   
 f)  $x^4 + (k-3)x^2 - 2(k-1)x + k = 0$   
 g)  $x^4 + 4kx^3 + 27k^2 = 0$   
 h)  $x^5 - 5k^2x^3 + 10k^4x + k^5 = 0$   
 i)  $x^5 + 5kx^4 + 4k^2 = 0$   
 j)  $x^4 - 3kx^2 + (3k^2 - 9)x + 9k - k^3 = 0$   
 k)  $x^4 + 4kx^3 + 27k^2 = 0$
- 3  $x^3 + 3ax + b = 0$  has a multiple root if and only if  $4a^3 + b^2 = 0$ .
- 4 If  $x^3 + 3ax^2 + 3bx + c = 0$  has a multiple root, then either  $b = a^2$  and  $-a$  is a triple root, or  $b \neq a^2$  and  $\frac{(ab - c)}{2(b - a)}$  is a double root.
- 5 If  $f(x)$  is of degree  $n$ ,  $f(x)$  and  $f'(x)$  cannot have more than  $\frac{1}{2}n$  distinct common roots.
- 6 If  $f(x)$  is irreducible over  $\mathbb{F}$ , all its roots are simple.
- 7 If  $f(x)$  is in  $\mathbb{F}[x]$  and has a single multiple root, the other roots, if any, being simple, then that root is in  $\mathbb{F}$ .
- 8 If  $f(x)$  is a cubic polynomial in  $\mathbb{F}[x]$  and has a multiple root, then all the roots of  $f(x)$  are in  $\mathbb{F}$ .
- 9 If  $f(x)$  is not a constant and every root of  $f'(x)$  is a root of  $f(x)$ , then all the roots of  $f(x)$  are equal.
- 10 If  $p \neq 0$ ,  $x^5 + 5px^3 + 5p^2x + 2q = 0$  has no root whose multiplicity exceeds two.
- 11 Show that 1 is a simple root of  $x^n + nx^{n-1} + nx^{n-2} + \dots + 1 = 0$ ,  $n > 2$ .
- 12 a) Show that 1 is a simple root of  $x^n + x^2 - x - 1 = 0$ ,  $n > 2$ .  
 b) For what values of  $n$  is  $-1$  a multiple root?
- 13 Show that the following have no multiple roots.
- a)  $(1+x)^n + (1-x)^n = 0$ ,  $n \geq 1$   
 b)  $x^n + 2nx^{n-1} + 1 = 0$ ,  $n \geq 2$   
 c)  $x^n + x^{n-2} + 1 = 0$ ,  $n \geq 2$
- 14 If  $n > 1$  then  $x^n + 2nax^{n-1} + nb = 0$  has a multiple root if and only if  $b = 0$  or  $b = na^2$ .
- 15 Find  $a$ ,  $b$  and  $n$  so that 1 shall be a triple root of  $x^n + n(n-1)ax^2 + nbx - 3 = 0$ ,  $n \geq 3$ .
- 16 If  $n > 2$ , find all values of  $a$  for which  $x^n + nax^2 - (n-2)a = 0$  has a multiple root.

- 17 If  $n > 1$ ,  $(n-1)x^n - nax^{n-1} + b = 0$  has a multiple root if and only if  $b = 0$  or  $b = a^n$ .
- 18 Find all integral values of  $a$  for which  $x^n + n(n-1)x^2 - 2n(n-2)ax + (n-1)(n-2)a^2 = 0$ ,  $n > 2$ , has a multiple root.
- 19 If  $n > 1$ ,  $(x+1)^n - x^n - 1 = 0$  has a multiple root if and only if  $n-1$  is divisible by 6. In this case the multiple roots are the imaginary cube roots of 1 and each is a double root.
- 20 Let  $f(x)$  be a non-constant polynomial in  $\mathfrak{F}[x]$ ,  $p_1^{i_1}(x)p_2^{i_2}(x) \cdots p_k^{i_k}(x)$  its factorization into primes in  $\mathfrak{F}[x]$ , no two of the primes associates. Prove:
- The multiplicity of each root of  $f(x)$  is one of the numbers  $i_1, i_2, \dots, i_k$ . (Hint: Use ex. 6 above and ex. 9, §6, Ch. 3.)
  - If  $r_1, r_2, \dots, r_i$  are all the distinct roots of  $f(x)$  of multiplicity  $i$  (where  $i$  is one of  $i_1, i_2, \dots, i_k$ ), then  $(x-r_1)(x-r_2) \cdots (x-r_i)$  is in  $\mathfrak{F}[x]$ .
- 21 If  $f(x)$  is in  $\mathfrak{F}[x]$  and one root has a multiplicity different from that of all the others, then that root is in  $\mathfrak{F}$ . (Hint: Use ex. 20. Ex. 7 is a special case.)
- 22 If  $f(x)$  is in  $\mathfrak{F}[x]$  and  $f(x) = g^m(x)$ , where  $m$  is a positive integer and  $g(x)$  has leading coefficient 1, then  $g(x)$  is in  $\mathfrak{F}[x]$ . (Hint: Use ex. 20.)

**3. Expansions of polynomials** Let  $f(x)$  be a polynomial whose degree, if any, does not exceed the integer  $n \geq 0$ . Let  $r_1, r_2, \dots, r_n$  be  $n$  complex numbers, not necessarily all distinct (if  $n = 0$  there are no  $r$ 's). Then (ex. 17, §4, Ch. 2)  $f(x)$  is uniquely expressible in the form

$$f(x) \equiv c_0 + c_1(x-r_1) + c_2(x-r_1)(x-r_2) + \cdots + c_n(x-r_1)(x-r_2) \cdots (x-r_n)$$

where  $c_0, c_1, \dots, c_n$  are constants.

One way to obtain the  $c_i$  is to multiply out the expressions on the right side, collect terms involving like powers of  $x$ , and equate coefficients of like powers of  $x$  on both sides of the equation. From the resulting equations we can then determine  $c_n, c_{n-1}, \dots, c_1, c_0$  successively. This is straightforward but laborious.

Another and simpler way is by successive application of the division algorithm (§6, Ch. 2). Observe that if  $f(x)$ , as expressed above, is divided by  $x-r_1$  the quotient is  $f_1(x) \equiv c_1 + c_2(x-r_2) + c_3(x-r_2)(x-r_3) + \cdots + c_n(x-r_2)(x-r_3) \cdots (x-r_n)$  and the remainder is  $c_0$ .

If  $f_1(x)$  be divided by  $x - r_2$  the quotient is  $f_2(x) \equiv c_2 + c_3(x - r_3) + \dots + c_n(x - r_3)(x - r_4) \dots (x - r_n)$  and the remainder is  $c_1$ .

Continuing this, we see that  $c_0, c_1, \dots, c_{n-1}$  are the successive remainders as we divide  $f(x)$  and the successive quotients by  $x - r_1, x - r_2, \dots, x - r_n$  respectively. By comparing the  $x^n$  terms, we see that  $c_n$  is the leading coefficient of  $f(x)$ .

*Example* Express  $f(x) = 4x^3 - 7x^2 + 2x - 1$  in the form  $c_0 + c_1x + c_2x(x - 1) + c_3x(x - 1)(x - 2)$ .

Here  $n = 3, r_1 = 0, r_2 = 1, r_3 = 2$ .

If we perform the indicated operations in the desired expression and collect terms involving like powers of  $x$ , then

$$4x^3 - 7x^2 + 2x - 1 = c_3x + (-3c_3 + c_2)x^2 + (2c_3 - c_2 + c_1)x + c_0$$

By equating coefficients,  $c_3 = 4, -3c_3 + c_2 = -7, 2c_3 - c_2 + c_1 = 2, c_0 = -1$ . From these we obtain  $c_3 = 4, c_2 = 5, c_1 = -1, c_0 = -1$ , so that

$$f(x) = -1 - x + 5x(x - 1) + 4x(x - 1)(x - 2)$$

If we proceed by the second method above, we have

$$\begin{array}{rcl} 4 & -7 & 2 & -1 & \underline{0} \\ & 0 & 0 & 0 & \\ \hline 4 & -7 & 2 & -1 & = c_0 & \underline{1} \\ & 1 & -3 & & \\ \hline 4 & -3 & -1 & & = c_1 & \underline{2} \\ & 8 & & & \\ \hline 4 & & 5 & & = c_2 \\ \hline 4 & & & & = c_3 \end{array}$$

**4. Taylor expansion** One of the most useful expansions of a polynomial is the type in which the  $r_1, r_2, \dots, r_n$  are all equal. In this case the expansion has the form

$$f(x) \equiv c_0 + c_1(x - h) + c_2(x - h)^2 + \dots + c_n(x - h)^n$$

where  $c_0, c_1, \dots, c_n$  are constants

This is called the Taylor expansion of  $f(x)$  in powers of  $x - h$ . For  $h = 0$  it is the usual form in which a polynomial is written.



The desired result now follows immediately by letting  $x = h$  in these equations.

### Exercises

1 Expand in powers of  $x - h$ :

a)  $2x^4 + x^2 - 5x + 2$ ,  $h = -1$

b)  $x^4 - 12x^3 + 216x - 405$ ,  $h = 3$

c)  $x^3 + 13x + 2$ ,  $h = 2i$

d)  $x^4 + (8i - 4)x^3 - (18 + 24i)x^2 + (44 - 8i)x + 24i - 7$ ,  $h = 1 - 2i$

e)  $9x^3 - 9x^2$ ,  $h = \frac{1}{3}$

2 Express the given polynomial in the specified form:

a)  $x^3$ ;  $c_0 + c_1x + c_2x(x+1) + c_3x(x+1)(x+2)$

b)  $x^3 - 1$ ;  $c_0 + c_1(x+1) + c_2(x+1)(x-2) + c_3(x+1)(x-2)(x-3)$

c)  $x^4 - 2x^3 - x^2$ ;  $c_0 + c_1(x-1) + c_2(x+1)(x-1) + c_3(x+1)^2(x-1) + c_4(x+1)^2(x-1)^2$

d)  $x^4 - x^3 + 3x^2 - 2x + 1$ ;  $c_0 + c_1x + c_2x^2 + c_3x^2(x-1) + c_4x^2(x^2-1)$

e)  $x^4 - x^3 - 1$ ;  $c_0 + c_1(x+i) + c_2(x^2+1) + c_3(x^2+1)(x+i) + c_4(x^2+1)^2$

3 Prove: If  $f(x) = c_0 + c_1(x-h) + c_2(x-h)^2 + \cdots + c_n(x-h)^n$ , then the roots of  $c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$  are the roots of  $f(x)$  each diminished by  $h$ . (See ex. 6, §5, Ch. 3)

4 Using the result of ex. 3 find (by successive synthetic divisions) a polynomial whose roots are the roots of the given polynomial each diminished or increased as indicated:

a)  $x^4 - x^3 + 2x^2 + 1$ , diminished by 3

b)  $x^4 - x^3 + 2x^2 + 1$ , increased by 1

c)  $2x^3 - x^2 - 2x + 3$ , increased by 4

d)  $2x^3 - x^2 - 2x + 3$ , diminished by 2

e)  $x^4 - 2x^3 + 3x^2 - 2x + 2$ , diminished by  $i$

f)  $2x^4 - 3x^2 + 7x - 1$ , increased by 2

5 If  $g(x)$  is of degree  $n$ , every polynomial of degree  $n$  or less is uniquely expressible in the form  $c_0g^{(n)}(x) + c_1g^{(n-1)}(x) + \cdots + c_{n-1}g'(x) + c_ng^{(0)}(x)$ . [The Taylor expansion in powers of  $x - h$  is a special case with  $g(x) = (x - h)^n$ .]

6 Let  $g(x) = x^3 - x + 2$ . Express  $6x^3 + 3x^2 + 4$  in the form described in ex. 5.

7 If  $h_0, h_1, \dots, h_n$  are complex numbers,  $h_n \neq 0$ , there is a unique polynomial  $f(x)$  of degree  $n$  such that  $f(x), f'(x), \dots, f^{(n)}(x)$  are equal to  $h_0, h_1, \dots, h_n$  respectively for  $x = h$ .

8 If  $f(x)$  is of degree  $n$  and has real coefficients,  $h$  is real, and  $f(h) \geq 0, f'(h) \geq 0, \dots, f^{(n)}(h) \geq 0$ , then  $f(x)$  has no real root greater than  $h$ .

## POLYNOMIALS WITH REAL COEFFICIENTS

Unless otherwise stated, all polynomials considered in this chapter will be understood to have real coefficients. We denote the field of all real numbers by  $\mathcal{R}$ .

**1. Factorization** We have seen (§12, Ch. 2) that a polynomial with coefficients in a field  $\mathfrak{F}$  is uniquely factorable into polynomials with coefficients in  $\mathfrak{F}$  and irreducible over  $\mathfrak{F}$ . For further information concerning the factorization of polynomials in  $\mathcal{R}[x]$ , we should like to know what polynomials are irreducible over  $\mathcal{R}$ .

We have already seen that every linear polynomial is irreducible (§12, Ch. 2). A quadratic polynomial over  $\mathcal{R}$  is reducible over  $\mathcal{R}$  if and only if it has a linear factor with real coefficients; hence if and only if it has a real root. Thus the quadratic polynomials irreducible over  $\mathcal{R}$  are those which have no real roots.

Are there any other polynomials irreducible over  $\mathcal{R}$ ? We shall show that the answer is no. To do this we shall first prove two other theorems which are useful in several connections.

### THEOREM

*If  $f(x) \neq 0$  and  $g(x)$  are in  $\mathfrak{F}[x]$ ,  $g(x)$  irreducible over  $\mathfrak{F}$ , and  $f(x)$  and  $g(x)$  have a common root, then  $f(x) \equiv g^n(x)h(x)$  where  $n$  is a positive integer,  $h(x)$  is in  $\mathfrak{F}[x]$ , and  $g(x)$  and  $h(x)$  have no common root.*

*Proof:* Let  $D(x)$  be a H.C.F. of  $f(x)$  and  $g(x)$  in  $\mathfrak{F}[x]$ . Every common root of  $f(x)$  and  $g(x)$  is a root of  $D(x)$  (§6, Ch. 3). Since  $f(x)$  and  $g(x)$  have a common root,  $D(x)$  is of degree at least one. But  $g(x)$  is irreducible over  $\mathfrak{F}$ , so that its only factors in  $\mathfrak{F}[x]$  are constants and associates (§11, Ch. 2). Since  $D(x)$  is not a constant, it is an associate of  $g(x)$ .

Since  $D(x)$  is a factor of  $f(x)$ ,  $g(x)$ , which is an associate of  $D(x)$ , is also a factor of  $f(x)$ .

Let  $n$  be the highest power of  $g(x)$  which divides  $f(x)$ . Then  $f(x) \equiv g^n(x)h(x)$  where  $h(x)$  is in  $\mathfrak{R}[x]$  (§7, Ch. 2).

$g(x)$  and  $h(x)$  have no common root, for if they did have, then the same argument as before would show that  $h(x)$  is divisible by  $g(x)$ . But, by the definition of  $n$ , this is impossible.

### THEOREM

*If  $f(x) \neq 0$  has real coefficients and a root  $a + bi$ , where  $a$  and  $b$  are real and  $b \neq 0$ , of multiplicity  $k$ , then  $a - bi$  is a root of  $f(x)$  of multiplicity  $k$ .*

*Proof:*  $g(x) = [x - (a + bi)][x - (a - bi)] \equiv x^2 - 2ax + a^2 + b^2$  has real coefficients and, since it has no real root, is irreducible over  $\mathfrak{R}$ .

Since  $f(x)$  and  $g(x)$  have the common root  $a + bi$ , by the preceding theorem

$$f(x) \equiv g^n(x)h(x) \equiv [x - (a + bi)]^n[x - (a - bi)]^n h(x)$$

where  $h(x)$  has real coefficients and has neither  $a + bi$  nor  $a - bi$  as a root.

Since  $a + bi$  is a root of  $f(x)$  of multiplicity  $k$ , therefore  $n = k$ . Hence  $a - bi$  is also a root of  $f(x)$  of multiplicity  $k$ , and the theorem is proved.

### THEOREM

*If  $f(x)$  of degree  $n > 2$  has real coefficients,  $f(x)$  is reducible over  $\mathfrak{R}$ .*

*Proof:* By the fundamental theorem of algebra  $f(x)$  has a root  $r$ . By the factor theorem,  $x - r$  is a factor of  $f(x)$ .

If  $r$  is real, then  $f(x)$  has a factor with real coefficients. If  $r = a + bi$  is imaginary, then by the preceding theorem  $[x - (a + bi)][x - (a - bi)]$ , which has real coefficients, is a factor of  $f(x)$ .

In either case  $f(x)$  has a factor with real coefficients and of lower degree than  $f(x)$ . Hence  $f(x)$  is reducible over  $\mathfrak{R}$ , and the theorem is proved.

### THEOREM

*If  $f(x) \neq 0$  has real coefficients, it is uniquely expressible in the form  $af_1(x)f_2(x) \cdots f_p(x)$  where  $a$  is a real constant and each of the  $f_i(x)$*

has real coefficients with leading coefficient 1, and is of degree one or two, and is irreducible over  $\mathbb{R}$ .

*Proof:* This follows from the unique factorization theorem (§12, Ch. 2) and the fact that a polynomial irreducible over  $\mathbb{R}$  cannot be of degree greater than two.

**Example 1** Find a polynomial with real coefficients having  $1 + i$  as a double root.

If  $1 + i$  is to be a double root,  $1 - i$  must also be a double root. Therefore, the polynomial must have  $[x - (1 + i)]^2[x - (1 - i)]^2 \equiv x^4 - 4x^3 + 8x^2 - 8x + 4$  as a factor. Since this has real coefficients, this will serve as the desired polynomial.

**Example 2** Find the roots of  $f(x) \equiv x^4 + 2x^3 + 3x^2 + 2x + 2$ , given that  $i$  is a root.

Since the coefficients are real and  $i$  is a root,  $-i$  is also a root. Hence  $(x - i)(x + i) = x^2 + 1$  is a factor. By division,

$$f(x) \equiv (x^2 + 1)(x^2 + 2x + 2)$$

The roots of  $x^2 + 2x + 2$  are  $-1 + i$  and  $-1 - i$ . Thus the roots of  $f(x)$  are  $i, -i, -1 + i, -1 - i$ .

### Exercises

- 1 If  $f(x)$  of odd degree has real coefficients, it has a real root.
- 2 If the conjugate of every root of a polynomial with complex coefficients is a root of the same multiplicity, the coefficients are real.
- 3 Solve, using the given information:
  - a)  $x^4 + 4x^3 + 8x^2 + 16x + 16 = 0$ ,  $-2i$  is a root
  - b)  $4x^6 - 4x^5 - 18x^4 + 20x^3 - 34x^2 + 24x - 12 = 0$ ,  $\frac{1}{2}(1 + i)$  is a root
  - c)  $x^6 - 4x^5 + 9x^4 - 12x^3 + 12x^2 - 8x + 4 = 0$ ,  $1 - i$  is a double root
  - d)  $x^6 - 2x^5 + 2x^4 - x^3 + 2x - 2 = 0$ ,  $1 + i$  and  $-i$  are roots
  - e)  $x^3 - (2 + i)x^2 - 2(1 - i)x + 2i = 0$ ,  $i$  is a root
- 4 Form a polynomial with real coefficients such that
  - a)  $2 + i$  is a double root
  - b)  $1 + i$  is a simple root and  $i$  is a double root
  - c)  $-i$  is a triple root
  - d)  $2$  is a double root and  $1 - i$  a simple root
  - e)  $1 + \sqrt{2}i$  and  $1 - \sqrt{3}i$  are simple roots
- 5 If  $a$  and  $k$  are real, find them if:
  - a)  $x^5 + 7x^3 + 2x^2 + kx + 18 = 0$  has a root  $ai$
  - b)  $x^4 + kx^2 + 2kx + 4 = 0$  has a root  $a - ai$



- c)  $x^3 - 2ax^2 + 9x + k = 0$  has a root  $a + 3i$   
 d)  $x^4 + x^2 + x + k = 0$  has a root  $a + 3i$   
 e)  $x^3 + \lambda x^2 + 3x + 4k = 0$  has a root  $a + \sqrt{3}i$   
 f)  $x^4 - 4x^3 + ax^2 + kx + 4 = 0$  has a multiple imaginary root  
 g)  $x^4 - 4x^3 + 10ax^2 - 12ax + k = 0$  has a multiple imaginary root  
 6 If  $a, b, \alpha$  are real,  $x^3 + ax^2 + b = 0$  has an imaginary root  $\alpha + \alpha i$  if and only if  $b + 2a^3 = 0$ .

**2. Rational roots** We often have to find the roots of a polynomial  $f(x)$  whose coefficients are not only real but rational. If each of the coefficients be expressed in the form  $a/b$ , where  $a$  and  $b$  are integers, and  $c$  is an integer divisible by all the denominators, then  $g(x) \equiv cf(x)$  has integral coefficients and the same roots as  $f(x)$ . Hence, in seeking roots of polynomials with rational coefficients, it suffices to consider only polynomials with integral coefficients.

The simplest roots to look for are those which are themselves rational. But even though  $f(x)$  may have integral coefficients, it may not have any rational roots. However, if it has, they can be determined by means of the following theorem.

#### THEOREM

If  $f(x) \equiv a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ , where  $a_0, a_1, \dots, a_{n-1}, a_n$  are integers and  $a_0 \neq 0, a_n \neq 0$ , has a rational root  $p/q$ , where  $p$  and  $q$  are relatively prime integers, then  $p$  is a factor of  $a_n$  and  $q$  a factor of  $a_0$ .

*Proof:* Since  $p/q$  is a root of  $f(x)$ ,

$$a_0\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + \dots + a_{n-1}\left(\frac{p}{q}\right) + a_n = 0$$

Multiplying both sides by  $q^n$  and transposing terms, we have

$$\begin{aligned} a_0p^n &= -a_1p^{n-1}q - \dots - a_{n-1}pq^{n-1} - a_nq^n \\ &= q(-a_1p^{n-1} - \dots - a_{n-1}pq^{n-2} - a_nq^{n-1}) = qr \end{aligned}$$

Since  $a_1, a_2, \dots, a_n, p, q$  are integers,  $r$  is an integer. Since  $a_0p^n = qr$ ,  $q$  is a factor of  $a_0p^n$ . Since  $p$  and  $q$  are relatively prime,  $p^n$  and  $q$  are relatively prime (ex. 5, §10, Ch. 2, for integers). Hence  $q$  is a factor of  $a_0$  (ex. 9, §10, Ch. 2, for integers).

In a similar way, from  $a_nq^n = -a_0p^n - a_1p^{n-1}q - \dots - a_{n-1}pq^{n-1}$ , it follows that  $p$  is a factor of  $a_n$ .

**Example 1** Find the rational roots, if any, of  $f(x) \equiv 9x^4 - 6x^3 - 53x^2 + 36x - 6$ .

If there is a rational root it has the form  $p/q$  where  $p$  is a factor of  $-6$  and  $q$  a factor of  $9$ . Hence  $p$  is one of the integers  $\pm 1, \pm 2, \pm 3, \pm 6$  and  $q$  is one of  $\pm 1, \pm 3, \pm 9$ . Dividing all possible values of  $p$  by all possible values of  $q$ , the only possible rational roots are  $\pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{9}, \pm \frac{2}{9}$ .

By trial [finding  $f(r)$  as the remainder in the synthetic division of  $f(x)$  by  $x - r$ ], we find that  $\frac{1}{3}$  is a root and

$$f(x) \equiv 3(x - \frac{1}{3})(3x^3 - x^2 - 18x + 6)$$

Proceeding with  $g(x) \equiv 3x^3 - x^2 - 18x + 6$  as we did with  $f(x)$ , its only possible rational roots are  $\pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{3}, \pm \frac{2}{3}$ . Again,  $\frac{1}{3}$  is a root of  $g(x)$ , and  $f(x) \equiv 9(x - \frac{1}{3})^2(x^2 - 6)$ .

Thus, the roots of  $f(x)$  are  $\frac{1}{3}, \frac{1}{3}, \sqrt{6}, -\sqrt{6}$ .

**Example 2** Find all integral values of  $k$  for which  $x^3 - (k+1)x + 2k = 0$  has a rational root.

Since the coefficients are integers, every rational root has the form  $p/q$  where  $p$  and  $q$  are integers and  $q$  is a factor of  $a_0 = 1$ . Therefore,  $q$  is  $\pm 1$ , so that every rational root is an integer.

If  $x$  is a root, then

$$\begin{aligned} 2k - kx &= x - x^3 \\ k(x - 2) &= x^3 - x \end{aligned}$$

If  $x = 2$  then  $0 = 8 - 2$ , which is impossible. Hence  $x \neq 2$ , so that

$$k = \frac{x^3 - x}{x - 2} = x^2 + 2x + 3 + \frac{6}{x - 2}$$

If  $k$  and  $x$  are integers,  $6/(x - 2)$  is an integer. Hence,  $x - 2$  is an integral factor of  $6$ . Therefore,  $x - 2$  is one of the integers  $\pm 1, \pm 2, \pm 3, \pm 6$ , so that  $x$  is one of the integers  $1, 3, 0, 4, -1, 5, -4, 8$ . For these values of  $x$  the corresponding values of  $k$  are  $0, 21, 0, 30, 0, 10, 10, 81$ .

**Example 3** Prove that  $\sqrt{2} + \sqrt{3}$  is irrational.

If  $x = \sqrt{2} + \sqrt{3}$ , then  $x - \sqrt{2} = \sqrt{3}$ . Squaring both sides and transposing terms,  $x^2 - 1 = 2\sqrt{2}x$ . Squaring again and simplifying,  $x^4 - 10x^2 + 1 = 0$ .

Thus,  $x$  is a root of a polynomial with rational coefficients.

The only possible rational roots are  $\pm 1$ , and neither is a root.

Hence,  $x$  is not rational.

### Exercises

1 Find the rational roots and, if possible, solve:

a)  $9x^4 + 9x^3 + 8x^2 - x - 1 = 0$

b)  $x^3 - 7x^2 + 2x - 3 = 0$

c)  $9x^4 - 12x^3 + 13x^2 - 12x + 4 = 0$

d)  $8x^5 + 12x^4 + 14x^3 + 13x^2 + 6x + 1 = 0$

e)  $2x^4 - 2x^3 + 7x^2 - x + 3 = 0$

f)  $9x^6 + 12x^5 + 40x^4 + 4x^3 + 52x^2 + 48x + 16 = 0$

g)  $4x^6 + 4x^5 + 9x^4 + 8x^3 + 6x^2 + 4x + 1 = 0$

h)  $2x^4 - 7x^3 + 14x^2 - 28x + 21 = 0$

i)  $4x^4 - 4x^3 + 37x^2 - 36x + 9 = 0$

2 If  $f(x)$  has integral coefficients and leading coefficient 1, every rational root is an integer and a factor of the constant term.

3 Find the integral values of  $k$ , if any, for which there is a rational root, and for these values of  $k$  find the rational roots:

a)  $x^3 + kx^2 + kx + 2 = 0$

b)  $x^3 + (2 - k)x^2 + (2k + 3)x - 6 = 0$

c)  $x^4 - 4x^3 - kx^2 + 6kx + 9 = 0$

d)  $x^3 - 3kx^2 + kx + 4 = 0$

e)  $x^4 - 3x^3 + kx^2 - 4x - 1 + k = 0$

f)  $x^3 + x^2 + kx + k = 0$

g)  $2x^3 - kx^2 + 2x - 1 = 0$

h)  $2x^3 - x^2 + 2(k - 1)x - k = 0$

i)  $kx^3 + (k - 1)x^2 - 1 = 0$

j)  $kx^3 - kx - 1 = 0$

4 If  $x^3 + ax^2 + bx + c$ , where  $a, b, c$  are integers, is reducible over the field of rational numbers, it is the product of a linear and quadratic factor each with integral coefficients.

5 Prove the following irrational:

a)  $\sqrt{5} - 3\sqrt{2}$

d)  $\sqrt{2} - \sqrt[3]{3}$

b)  $\sqrt{2} + \sqrt[3]{2}$

e)  $\sqrt{2} + \sqrt[3]{3}$

c)  $\sqrt{2} + \sqrt[3]{3}$

f)  $\sqrt[n]{n^2} + 1, n \text{ a non-zero integer}$

6 If  $a$  and  $b$  are integers, find them under the conditions given and solve the equations:

a)  $x^3 + ax^2 + bx - 1 = 0$  has a double rational root

b)  $x^4 + ax^2 + bx - 3 = 0$  has a multiple rational root

c)  $x^3 + ax^2 + bx - 3 = 0$  has only rational roots

- 7 If  $a, b, c$  are integers, find them, and the rational roots, under the conditions given:
- $x^5 + ax^3 + bx^2 + cx + 4 = 0$  has a rational root of multiplicity three
  - $x^4 + ax^3 + bx^2 + cx + 5 = 0$  has only rational roots
- 8 If  $a$  and  $b$  are rational,  $x^3 - 3x^2 + 3x - 3$  and  $x^3 - 3x^2 + ax + b^2$  are relatively prime.
- 9 Show that the following have no rational roots:
- $x^n - 3kx^2 + x^2 - 1 = 0, n > 2, k$  an integer
  - $x^n + 2kx + 2 = 0, n \geq 2, k$  an integer
  - $x^n + 3x^{n-1} - 18 = 0, n > 2$
  - $x^4 + x^3 + 2^n = 0, n \geq 1$
- 10 If  $n \geq 1, x^n + (1+x)^n + (1-x)^n = 0$  has a rational root if and only if  $n = 1$ .
- 11 If  $x$  is rational and  $2x^4 + 3x + 1$  is an integer,  $x$  is an integer.
- 12 If  $f(x)$  has integral coefficients and  $f(0)$  and  $f(1)$  are odd,  $f(x)$  has no integral root.
- 13 If  $f(x)$  has integral coefficients and  $p$  is a positive prime integer and none of  $f(0), f(1), \dots, f(p-1)$  is divisible by  $p$ , then  $f(x)$  has no integral root. [Hint: Suppose there is an integral root  $r = qp + s$  where  $0 \leq s < p$  and consider  $f(s)$ . Exercise 12 is a special case with  $p = 2$ .]
- 14 Prove: If  $a$  is a prime integer,  $x^n - a$  is irreducible over the field of rational numbers. (Hint: Suppose there is a factor with the roots  $r_1, r_2, \dots, r_m$ . Then  $r = r_1 r_2 \cdots r_m$  is rational and  $r^n = a^m$ . Hence  $r$  is a rational root of  $x^n - a^m$ , which is impossible if  $m < n$ . This result shows that over the rational field there are irreducible polynomials of all degrees.)
- \*15 Let  $n$  be a positive prime integer,  $\mathfrak{F}$  the rational field,  $a$  in  $\mathfrak{F}$ , and no  $n$ th root of  $a$  in  $\mathfrak{F}$ . Prove:  $x^n - a$  is irreducible over  $\mathfrak{F}$ . [Hint: As in ex. 14,  $r^n = a^m$ . If  $0 < m < n$  then  $\lambda n + \mu m = 1$  where  $\lambda, \mu$  are integers (§13, Ch. 2). Show  $a = (a^\lambda r^\mu)^n$ .] Show that the proof applies if  $\mathfrak{F}$  is any field.

**3. Conjugate square roots** Analogous to the result of §1 which says that the conjugate of an imaginary root of a polynomial with real coefficients is also a root, we have:

#### THEOREM

If  $f(x)$  has rational coefficients and a root  $a + \sqrt{b}$  of multiplicity  $k$ , where  $a$  and  $b$  are rational and  $\sqrt{b}$  is not, then  $a - \sqrt{b}$  is also a root of  $f(x)$  of multiplicity  $k$ .

Here  $\sqrt{b}$  may denote either square root of  $b$ .

*Proof:*  $g(x) \equiv [x - (a + \sqrt{b})][x - (a - \sqrt{b})] \equiv x^2 - 2ax + a^2 - b$  has rational coefficients and, we say, is irreducible over the rational field. For, if it were reducible, it would have a linear factor with rational coefficients and, therefore, a rational root. But neither  $a + \sqrt{b}$  nor  $a - \sqrt{b}$  is rational; for if  $a \pm \sqrt{b} = r$  were rational then  $\sqrt{b} = \pm(r - a)$  would also be rational.

We leave it to the reader to complete the proof as in §1.

### Exercises

1 Solve the following equations, using the given information:

a)  $2x^4 - x^3 - 12x^2 - 16x - 8 = 0$ ,  $1 + \sqrt{5}$  is a root

b)  $x^6 - 4x^5 + 4x^4 - 4x^3 + 5x^2 + 8x + 2 = 0$ ,  $1 - \sqrt{2}$  is a multiple root

c)  $x^6 - 7x^5 + 5x^4 + 32x^3 + x^2 - 81x + 21 = 0$ ,  $2 + \sqrt{3}$  and  $3 + \sqrt{2}$  are roots

d)  $x^6 - 4x^5 + 4x^4 - 8x^3 + 8x^2 - 16x + 8 = 0$ ,  $2 - \sqrt{2}$  is a root

e)  $x^7 - 5x^6 + 12x^4 - 7x^3 + 23x^2 - 6x - 42 = 0$ ,  $\sqrt{3}$  and  $3 + \sqrt{2}$  are roots

2 Form a polynomial with rational coefficients such that

a)  $3 - \sqrt{7}$  is a double root

b)  $7 + \sqrt{3}$  is a simple root and  $\sqrt{3}$  a double root

c)  $-\sqrt{2}$  is a triple root

d)  $1 + \sqrt{5}$  and  $-1 + \sqrt{5}$  are simple roots

e)  $1 + \sqrt{2}$  and  $(1 + \sqrt{2})^2$  are simple roots

3 Prove: If  $f(x)$  has rational coefficients and a root  $\sqrt{a} + \sqrt{b}$  of multiplicity  $k$ , where  $a$  and  $b$  are rational and  $\sqrt{a}$ ,  $\sqrt{b}$ ,  $\sqrt{a}\sqrt{b}$  are not, then each of  $\sqrt{a} - \sqrt{b}$ ,  $-\sqrt{a} + \sqrt{b}$ ,  $-\sqrt{a} - \sqrt{b}$  is a root of multiplicity  $k$ .

4 Solve the following, using ex. 3 and the given information:

a)  $x^5 - x^4 - 22x^3 + 22x^2 + 25x - 25 = 0$ ,  $2\sqrt{2} - \sqrt{3}$  is a root

b)  $x^6 - 1715x^2 + 2058 = 0$ ,  $\sqrt{14} - \sqrt{7}$  is a root

c)  $x^6 + x^5 - 35x^4 - 36x^3 + 36x + 36 = 0$ ,  $\sqrt{6} + \sqrt{12}$  is a root

d)  $x^5 - x^4 + 117x^3 - 2x^2 - 242x - 121 = 0$ ,  $\sqrt{5} - i\sqrt{6}$  is a root

e)  $288x^5 - 144x^4 - 816x^3 + 408x^2 + 2x - 1 = 0$ ,  $\sqrt[3]{2} + \sqrt[3]{4}$  is a root

5 Find a polynomial with rational coefficients having a root

a)  $\sqrt{2} + \sqrt{5}$

d)  $i$  and a root  $\sqrt{10} + \sqrt{7}$

b)  $2\sqrt{3} + 3\sqrt{2}$

e)  $\sqrt{2} - 2i\sqrt{3}$

c)  $\sqrt{6} - \sqrt{5}$  and a root 1

- 6 If  $a$  and  $b$  are rational, find them and the roots if:
- $1 - \sqrt{5}$  is a root of  $2x^3 + ax^2 + bx - 4 = 0$
  - $3 + 2\sqrt{3}$  is a root of  $3x^3 + ax^2 + bx + 2b = 0$
  - $a + \sqrt{2}$  is a root of  $x^3 - 3ax^2 + bx - 2a = 0$
  - $2 + \sqrt{5}$  is a root of  $x^4 + ax^3 + ax + b = 0$
  - $a \neq 0$  and  $1 + a\sqrt{2}$  is a root of  $x^4 - 76x + b = 0$
- 7 If  $a$  and  $b$  are rational and  $\sqrt{a}$  is not, find  $a$ ,  $b$  and the roots if:
- $3 + \sqrt{a}$  is a root of  $2x^3 - 8x^2 - 12x + b = 0$
  - $1 + \sqrt{a}$  is a root of  $x^3 + bx^2 + x + 2b^2 = 0$
  - $a + \sqrt{a}$  is a root of  $x^3 - ax^2 + 5ax + b = 0$
  - $b + \sqrt{a}$  is a root of  $x^4 - 2(b+3)x^3 + 14x^2 + 46x + 7(a-b^2) = 0$
- 8 If  $a$ ,  $b$ ,  $c$  are rational,  $x^3 + ax^2 + bx + c = 0$  has a root  $p + \sqrt{q}$ , where  $p$  and  $q$  are rational, if and only if it has a rational root.
- 9 If  $a$  and  $b$  are integers, find them and the roots if  $x^3 + ax^2 + bx + 1 = 0$  has a root  $\frac{1}{2} + \sqrt{\alpha}$  where  $\alpha$  is rational and  $\sqrt{\alpha}$  is not.
- 10 If  $a$  is rational and  $x^3 + ax - 4 = 0$  is satisfied by  $\alpha + \sqrt{\beta}$  and  $\beta + \sqrt{\alpha}$  where  $\alpha$  and  $\beta$  are rational and  $\sqrt{\alpha}$  and  $\sqrt{\beta}$  are not, find  $a$  and the roots.
- 11 If  $p$  and  $q$  are rational,  $x^3 + px^2 + q = 0$  has a root  $a + \sqrt{a}$ , where  $a$  is rational and  $\sqrt{a}$  is not, if and only if  $q = -\frac{2}{27}(p+2)^2(2p+1)$  and  $\sqrt{(-1-2p)/3}$  is not rational.
- 12 If  $a$ ,  $b$ ,  $c$ ,  $d$  are rational and  $\sqrt{d}$  is not, and  $c + \sqrt{d}$  is a multiple root of  $x^4 + 4x^3 + ax^2 + bx + 4 - a = 0$ , find  $a$ ,  $b$ ,  $c$ ,  $d$ .
- 13 If  $a$ ,  $b$ ,  $c$  are rational and  $x^5 - 3x^4 + ax^3 + bx^2 + cx + 1 = 0$  has a double root  $d + \sqrt{e}$ , where  $d$  and  $e$  are integers and  $\sqrt{e}$  is not rational, find  $a$ ,  $b$ ,  $c$ ,  $d$ ,  $e$ .
- 14 If  $f(x)$  has rational coefficients, and  $a$  and  $b$  are rational and  $\sqrt[3]{b}$  is not, and  $a + \sqrt[3]{b}$  is a root of  $f(x)$ , then  $a + r_1$ ,  $a + r_2$ ,  $a + r_3$  are roots of  $f(x)$ , where  $r_1$ ,  $r_2$ ,  $r_3$  are the three cube roots of  $b$ .
- 15 If  $p$  and  $q$  are rational and  $\sqrt[3]{q}$  is not, and  $p$  and  $p + \sqrt[3]{q}$  are roots of  $x^4 + ax^3 + bx + c = 0$ , where  $a$ ,  $b$ ,  $c$  are rational, then  $a = c = 0$ . (Use ex. 14.)

**4. Location principle** If  $f(x)$  is a real function of a real variable, we can obtain some idea of the values of  $x$  for which  $f(x)$  vanishes by graphing the function and estimating the abscissas of the points where the graph meets the  $x$  axis. In general, it is impossible to plot all the points of the graph. The usual procedure is to plot enough points to obtain a good idea of the graph, and then to draw a smooth curve through them.

If the graph contains points on opposite sides of the  $x$  axis, we conclude that the graph crosses the  $x$  axis somewhere.

This conclusion is not always justified, but it is for the so-called continuous functions (including polynomials; see ex. 21, §4, Ch. 2). A proof of the general result will be found in texts on advanced calculus. For polynomials, which are relatively simple functions, we give a proof based upon the fundamental theorem of algebra.

We state the result as follows:

#### THEOREM

*If  $f(x)$  has real coefficients and  $a$  and  $b$  are real numbers such that  $f(a)$  and  $f(b)$  have opposite signs, then  $f(x)$  has a root between  $a$  and  $b$ .*

*Proof:* Since  $f(a) \neq f(b)$ ,  $a \neq b$ . Suppose, to be specific,  $a < b$ .

Since  $f(x)$  is not a constant, it follows (as a consequence of the fundamental theorem of algebra) that  $f(x) \equiv (f_1(x)f_2(x) \cdots f_r(x))$  where each of the  $f_i(x)$  is linear or quadratic, with real coefficients and leading coefficient 1, irreducible over the field of real numbers, and  $c$  is a non-zero real constant.

If  $f_j(x)$  is quadratic, then (§1) its roots are conjugate imaginaries; hence

$$f_j(x) = [x - (\alpha + \beta i)][x - (\alpha - \beta i)] \equiv (x - \alpha)^2 + \beta^2$$

Since  $\beta \neq 0$ ,  $f_j(x)$  is positive for every real value of  $x$ .

If  $f_j(x)$  is linear, we may write it in the form  $x - r$ , where  $r$  is a real root of  $f(x)$ . Since  $f(a)$  and  $f(b)$  are different from zero,  $r$  is neither  $a$  nor  $b$ . If  $r < a$  then  $x - r$  has the same signs for  $x = a$  and  $x = b$ . The same is true if  $r > b$ .

Let  $g(x)$  be the product of the constant  $c$ , all the quadratic factors in the factorization of  $f(x)$ , and all the linear factors  $x - r$  for which either  $r < a$  or  $r > b$ . Then

$$f(x) \equiv (x - r_1) \cdots (x - r_l)g(x)$$

where  $r_1, \dots, r_l$  are the remaining real roots of  $f(x)$ , if any, i.e., those which lie between  $a$  and  $b$ , and  $g(x)$  has the same signs for  $x = a$  and  $x = b$ .

For every  $j$ ,  $a - r_j$  is negative and  $b - r_j$  is positive. Therefore,

$$f(a) = (a - r_1) \cdots (a - r_l)g(a) = (-1)^l \lambda g(a)$$

where  $\lambda$  is positive;

$$f(b) = (b - r_1) \cdots (b - r_k)g(b) = \mu g(b)$$

where  $\mu$  is positive.

Since  $\lambda$  and  $\mu$  have the same signs, and  $g(a)$  and  $g(b)$  have the same signs,  $f(a)$  and  $f(b)$  differ in sign if and only if  $k$  is odd. Hence,  $k$  is at least one, and the theorem is proved.

Actually the proof above shows that  $k$  is odd if  $f(a)$  and  $f(b)$  have opposite signs and even (possibly zero) if  $f(a)$  and  $f(b)$  have the same signs. Thus, if each root be counted as often as its multiplicity,  $f(x)$  has an odd number of roots between  $a$  and  $b$  if  $f(a)$  and  $f(b)$  have opposite signs and an even number (possibly none) if  $f(a)$  and  $f(b)$  have the same signs.

This highly useful result we shall refer to as the location principle.

**5. Sign for large values of  $x$**  If  $f(x)$  has real coefficients, we can try to determine whether it has any real roots, and to locate these roots, by seeking values of  $x$  for which the corresponding values of  $f(x)$  have opposite signs. Since there are many values of  $x$  which we can try, any means of limiting the trials is useful. In this connection the following is helpful.

#### THEOREM

If  $f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ , where  $a_0, a_1, \cdots, a_{n-1}, a_n$  are real and  $a_0 \neq 0$ , there exists an  $M \geq 0$  such that  $f(x)$  has the same sign as  $a_0x^n$  whenever  $x$  is real and  $|x| > M$ .

*Remark* Specifically, as we shall show,  $M$  may be taken as the largest of  $2|a_1/a_0|, 2\sqrt{|a_2/a_0|}, \cdots, 2\sqrt[n]{|a_n/a_0|}$ .

*Proof:* For  $x \neq 0$ ,

$$f(x) = a_0x^n \left( 1 + \frac{a_1}{a_0x} + \frac{a_2}{a_0x^2} + \cdots + \frac{a_n}{a_0x^n} \right)$$

Taking  $M$  as defined in the remark, we have

$$2\sqrt[i]{\frac{|a_i|}{|a_0|}} \leq M \quad \text{for } i = 1, 2, \cdots, n$$



so that

$$\left| \frac{a_1}{a_0} \right| \frac{1}{M} \leq \frac{1}{2}$$

For  $|x| > M$

$$\begin{aligned} \left| \frac{a_1}{a_0 x} + \frac{a_2}{a_0 x^2} + \cdots + \frac{a_n}{a_0 x^n} \right| &\leq \left| \frac{a_1}{a_0} \right| \frac{1}{|x|} + \left| \frac{a_2}{a_0} \right| \frac{1}{|x|^2} + \cdots \\ &\quad + \left| \frac{a_n}{a_0} \right| \frac{1}{|x|^n} \quad (\S 4, \text{Ch. 1}) \\ &< \left| \frac{a_1}{a_0} \right| \frac{1}{M} + \left| \frac{a_2}{a_0} \right| \frac{1}{M^2} + \cdots + \left| \frac{a_n}{a_0} \right| \frac{1}{M^n} \\ &\leq \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} \\ &= 1 - \frac{1}{2^n} < 1 \end{aligned}$$

When  $x$  is real and  $|x| > M$  this implies

$$-1 < \frac{a_1}{a_0 x} + \frac{a_2}{a_0 x^2} + \cdots + \frac{a_n}{a_0 x^n} < 1$$

so that  $1 + \frac{a_1}{a_0 x} + \frac{a_2}{a_0 x^2} + \cdots + \frac{a_n}{a_0 x^n}$  is positive, which establishes the desired result.

*Example* Show that all the roots of  $f(x) = x^3 + 3x^2 - 3$  are real and locate them between successive integers.

By the remark above,  $f(x)$  has the sign of  $x^3$  when  $x$  is real and  $|x| > 6$ . Hence,  $f(x)$  is positive for  $x > 6$  and negative for  $x < -6$ .

Since  $f(0) = -3$  and  $f(1) = 321$ , by the location principle  $f(x)$  has a root between 0 and 1. Since  $f(1) = 1$ , there is a root between 0 and 1.

Since  $f(0)$  and  $f(-6)$  are negative by the location principle  $f(x)$  has two or no negative roots. But  $f(-2) = 1$ , so that  $f(x)$  has a root between 0 and  $-2$  and a root between  $-2$  and  $-6$ . Since  $f(-1)$  and  $f(-3)$  are negative, there is a root between  $-1$  and  $-2$  and a root between  $-2$  and  $-3$ .

Thus,  $f(x)$  has three real roots, and we have located them between successive integers.

*Remark* The location principle by itself is usually not sufficient to determine the number or location of real roots. Thus, in the example, had we not succeeded in finding a negative value of  $x$  for which  $f(x)$  is positive, we would not have been able to decide whether  $f(x)$

has two or no negative roots. Later (Ch. 6) we shall develop other means of locating real roots.

### Exercises

#### 1 Show that:

- a)  $x^3 - 5x + 1 = 0$  has two positive roots and one negative root
- b)  $x^4 - 3x^3 - x^2 + 5x - 1 = 0$  has three positive roots and one negative root
- c)  $x^4 + 3x + 1 = 0$  has two negative and two imaginary roots
- d)  $x^3 + ax^2 + b = 0$  has one negative and two imaginary roots if  $a$  and  $b$  are positive
- e)  $x^4 - 12x + 1 = 0$  has two positive and two imaginary roots.

#### 2 If $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ has real coefficients, then:

- a) If  $n$  is even and  $a_0$  and  $a_n$  have opposite signs, there is at least one positive root and at least one negative root.
- b) If  $n$  is odd and  $a_0$  and  $a_n$  have opposite signs, there is at least one positive root.
- c) If  $n$  is odd and  $a_0$  and  $a_n$  have the same signs, there is at least one negative root.

#### 3 If $-11 < a < 97$ then $x^4 + 16x^3 - 44x^2 + 39x + a = 0$ has an odd number of roots, counting multiplicities, between $-1$ and $1$ .

#### 4 If $x^3 - 3x^2 + x + a = 0$ , $a \neq 0$ , has exactly one root (counting multiplicities) between $0$ and $1$ , then there is exactly one root between $2$ and $3$ .

#### 5 If $x^5 + ax^2 + 7$ has exactly one root, counting multiplicities, between $-1$ and $1$ , then that root is negative.

#### 6 If $x^4 - 2x^3 + 6x^2 - x + a$ has exactly one root, counting multiplicities, between $-2$ and $2$ , then that root is between $-1$ and $-2$ .

#### 7 If $f(x)$ has real coefficients, prove $f(x)$ has the same sign for all real values of $x$

- a) between two consecutive real roots of  $f(x)$ .
- b) greater than the greatest real root of  $f(x)$ .
- c) smaller than the smallest real root of  $f(x)$ .

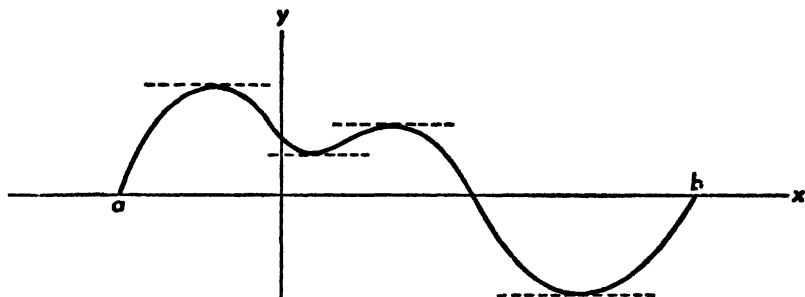
[Note: Real numbers  $a$  and  $b$  are said to be consecutive roots of  $f(x)$  if  $a \neq b$ ,  $f(a) = f(b) = 0$ , and  $f(x)$  has no root between  $a$  and  $b$ .]

#### 8 If $f(a) \neq f(b)$ and $\xi$ is a number between $f(a)$ and $f(b)$ , then there is a number $x_0$ between $a$ and $b$ such that $f(x_0) = \xi$ .

#### 9 If $f(x)$ has real coefficients, $f(a) \neq 0$ where $a$ is real, then there exists a positive number $\lambda$ such that $f(x)$ has the same sign as $f(a)$ whenever $x$ is real and $|x - a| < \lambda$ .

#### 10 Extend the result of ex. 9 in case $f(a) = 0$ to show that if $f^{(k)}(x)$ is the first of the derivatives $f'(x)$ , $f''(x)$ , $\cdots$ which does not vanish for $x = a$ then $f(x)$ has the same sign as $(x - a)^k f^{(k)}(a)$ when $x$ is real and $|x - a| < \lambda$ . (Exercise 9 is a special case with $k = 0$ .)

**6. Rolle's theorem** In the calculus the tangent line at a point  $(x_0, y_0)$  of the graph of a function of a real variable is defined and it is shown that the slope of the line is  $f'(x_0)$ . It is evident from the graph that if  $f(x)$  vanishes for  $x = a$  and  $x = b$ , where  $a \neq b$ , there is at least one value of  $x$  between  $a$  and  $b$  for which the tangent line at the corresponding point on the graph is horizontal. At such a point  $f'(x)$  vanishes.



This result is essentially Rolle's theorem. It is valid for functions which are continuous for all values of  $x$  between  $a$  and  $b$  inclusive and which are differentiable when  $x$  is between  $a$  and  $b$ . It applies, therefore, to polynomials with real coefficients.

For a proof of the general result we refer the reader to texts on advanced calculus. For polynomials we prove it as a corollary of a more general theorem.

#### THEOREM

*Suppose  $f(x)$ ,  $g(x)$ , and  $h(x)$  have real coefficients,  $a$  and  $b$  are consecutive real roots of  $f(x)$ , and  $g(a)$  and  $g(b)$  have the same signs. Then  $F(x) \equiv g(x)f'(x) + h(x)f(x)$  has an odd number of roots between  $a$  and  $b$  if each root be counted as often as its multiplicity.*

*Proof:* Since  $f(x)$  has no root between  $a$  and  $b$ ,  $f(x) \neq 0$ . Let  $a$  and  $b$  be roots of  $f(x)$  of multiplicities  $p$  and  $q$  respectively. Then

$$f(x) \equiv (x - a)^p(x - b)^q k(x)$$

where  $k(x)$  has real coefficients and has no root between  $a$  and  $b$  inclusive.

By the location principle,  $k(a)$  and  $k(b)$  have the same signs.

By the rules for differentiation,

$$\begin{aligned} f'(x) &\equiv p(x-a)^{p-1}[(x-b)^q k(x)] + (x-a)^p [(x-b)^q k(x)]' \\ &\equiv p(x-a)^{p-1}(x-b)^q k(x) + (x-a)^p [q(x-b)^{q-1} k(x) \\ &\quad + (x-a)^p (x-b)^q k'(x)] \\ &\equiv (x-a)^{p-1}(x-b)^{q-1} l(x) \end{aligned}$$

$$\text{where } l(x) \equiv p(x-b)k(x) + q(x-a)h(x) + (x-a)(x-b)k'(x).$$

Thus,

$$\begin{aligned} F(x) &\equiv g(x)(x-a)^{p-1}(x-b)^{q-1}l(x) + h(x)(x-a)^p(x-b)^q k(x) \\ &\equiv (x-a)^{p-1}(x-b)^{q-1}m(x) \end{aligned}$$

$$\text{where } m(x) \equiv g(x)l(x) + (x-a)(x-b)h(x)k(x).$$

We have

$$\begin{aligned} m(a) &= g(a)l(a) = p(a-b)g(a)k(a) \\ m(b) &= g(b)l(b) = q(b-a)g(b)k(b) \end{aligned}$$

Since  $k(a)$  and  $k(b)$  have the same signs, and  $g(a)$  and  $g(b)$  have the same signs, and  $p$  and  $q$  are positive, and  $a-b$  and  $b-a$  have opposite signs, therefore  $m(a)$  and  $m(b)$  have opposite signs.

By the location principle,  $m(x)$  has an odd number of roots between  $a$  and  $b$ . Therefore, the same is true of  $F'(x)$ , and the theorem is proved.

### COROLLARY

*(Rolle's theorem) Between two consecutive real roots of a polynomial  $f(x)$  with real coefficients  $f'(x)$  has an odd number of roots (counting multiplicities) and, therefore, at least one.*

*Proof:* Apply the theorem with  $g(x) \equiv 1$ ,  $h(x) \equiv 0$ .

*Example* Determine the number of roots of  $f(x) = 3x^3 + 6x^2 + 4x + 2$  between  $-1$  and  $-2$ .

Since  $f(-1)$  is positive and  $f(-2)$  is negative,  $f(x)$  has one or three roots between  $-1$  and  $-2$ .

But  $f'(x) \equiv 9x^2 + 12x + 4 \equiv (3x+2)^2$  has no root between  $-1$  and  $-2$ . Hence (theorem 2, §2, Ch. 4)  $f(x)$  has no multiple root between  $-1$  and  $-2$  nor (by Rolle's theorem) can it have two distinct roots between  $-1$  and  $-2$ .

Thus,  $f(x)$  has exactly one root between  $-1$  and  $-2$ .

## Exercises

$f(x)$ ,  $g(x)$ ,  $h(x)$  are polynomials with real coefficients.  $F(x) \equiv g(x)f'(x) + h(x)f(x)$ . Roots are to be counted as often as their multiplicities.

If  $a < b$ , the interval  $[a, b]$  means the set of all numbers between  $a$  and  $b$  inclusive, i.e., all values of  $x$  such that  $a \leq x \leq b$ .

- 1 If  $a$  and  $b$  are consecutive real roots of  $f(x)$  and  $g(a)$ ,  $g(b)$  have the same signs, then  $F(a)$  and  $F(b)$  do not have the same signs.
- 2 If  $g(x)$  has no real root, then between two consecutive real roots of  $F(x)$  there cannot be more than one root of  $f(x)$ .
- 3 If  $f(x)$  has  $k$  real roots and  $g(x)$  has no real root, then  $F(x)$  has at least  $k - 1$  real roots. From this, or from Rolle's theorem, deduce:
  - (a)  $f^{(i)}(x)$  has at least  $k - i$  real roots (b) the number of imaginary roots of  $f^{(i)}(x)$  cannot exceed the number of imaginary roots of  $f(x)$ .
- 4 If  $f(x)$  has  $k$  roots which exceed  $a$  and  $g(x)$  has no root which exceeds  $a$ , then  $F(x)$  has at least  $k - 1$  roots which exceed  $a$ . From this, or from Rolle's theorem, deduce: Not more than one root of  $f(x)$  exceeds the greatest real root of  $f'(x)$ .
- 5 If  $f(x)$  has  $k$  roots in the interval  $[a, b]$  and  $g(x)$  has none, then  $F(x)$  has at least  $k - 1$  roots in  $[a, b]$ .
- 6 If  $f(x)$  is of degree  $n$  and has  $n$  distinct real roots, then all the roots of  $f'(x)$  are real and simple.
- 7  $f(x)$  cannot have more than two roots between two consecutive real roots of  $f''(x)$ .

**7. Monotoneity** A real function  $f(x)$  of a real variable  $x$  is said to be monotonically increasing in a domain if  $f(x_1) < f(x_2)$  whenever  $x_1$  and  $x_2$  are values of  $x$  in the domain such that  $x_1 < x_2$ . Similarly, it is defined to be monotonically decreasing in the domain if  $f(x_1) > f(x_2)$  whenever  $x_1 < x_2$ .

It is shown in the calculus that if  $f'(x)$  is positive for all values of  $x$  in an interval then  $f(x)$  is monotonically increasing in the interval, and if  $f'(x)$  is always negative in the interval then  $f(x)$  is monotonically decreasing.

These theorems are evident geometrically. For if  $f'(x)$  is positive throughout an interval then the tangent line to the graph of  $f(x)$ , for any value of  $x$  in the interval, has positive slope and, therefore, slants upward and to the right; hence the graph rises as we move from left to right. A similar intuitive discussion applies if  $f'(x)$  is negative.

Rigorous demonstrations can be given by means of the theorem of the mean (also called the mean-value theorem) which can be proved from Rolle's theorem. We prove the mean-value theorem for polynomials and then establish the results about monotonicity.

### THEOREM

*If  $f(x)$  has real coefficients and  $a$  and  $b$  are distinct real numbers, there exists an  $x_0$  between  $a$  and  $b$  such that  $[f(b) - f(a)]/(b - a) = f'(x_0)$ .*

*Proof:* Let  $g(x) \equiv f(x) - f(a) - \frac{f(b) - f(a)}{b - a} (x - a)$

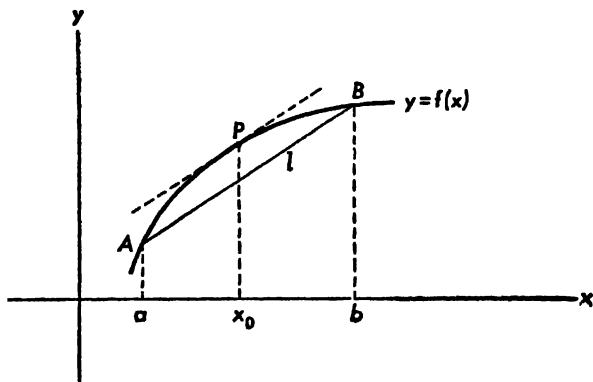
$g(x)$  has real coefficients and  $g(a) = g(b) = 0$ . By Rolle's theorem there is an  $x_0$  between  $a$  and  $b$  such that  $g'(x_0) = 0$ . But

$$g'(x) \equiv f'(x) - \frac{f(b) - f(a)}{b - a}$$

Hence 
$$g'(x_0) = f'(x_0) - \frac{f(b) - f(a)}{b - a}$$

Since  $g'(x_0) = 0$ , the theorem is proved.

*Remark* The mean-value theorem has a simple geometric interpretation. The points on the graph of  $f(x)$  with abscissas  $a$  and  $b$  are  $(a, f(a))$  and  $(b, f(b))$  respectively. The slope of the line  $l$  determined by these points is  $[f(b) - f(a)]/(b - a)$ . The mean-value theorem says that there is a point on the graph, with abscissa  $x_0$  between  $a$  and  $b$ , at which the tangent line (whose slope is  $f'(x_0)$ ) has the same slope as  $l$ ; i.e., the tangent line is parallel to the chord.



Incidentally, an equation for line  $l$ , in the point-slope form, is

$$y = f(a) + \frac{f(b) - f(a)}{b - a} (x - a)$$

Thus  $g(x)$  referred to in the proof above is the difference between the ordinate of any point on the graph and the ordinate of the point on line  $l$  with the same abscissa.

### THEOREM

*If  $f(x)$  has real coefficients and  $f'(x)$  is positive for every value of  $x$  between  $a$  and  $b$ , then  $f(x)$  is monotonically increasing in the interval  $a \leq x \leq b$ . If  $f'(x)$  is negative for every  $x$  between  $a$  and  $b$ ,  $f(x)$  is monotonically decreasing in the interval.*

*Proof:* Suppose  $f'(x)$  positive for  $a < x < b$ . The proof is similar if  $f'(x)$  is negative.

If  $a \leq x_1 < x_2 \leq b$  then, by the mean value theorem,

$$f(x_2) - f(x_1) = (x_2 - x_1)f'(x_0)$$

where  $x_1 < x_0 < x_2$ .

Since  $a < x_0 < b$ ,  $f'(x_0)$  is positive. Since  $x_2 - x_1$  is also positive,  $f(x_2) > f(x_1)$ , and the theorem is proved.

*Example* Find the domains in which  $f(x) = 8x^5 - 5x^4 + \frac{1}{2}$  is monotonically increasing and those in which it is monotonically decreasing.

To apply the theorem we seek the domains in which  $f'(x)$  is positive and those in which it is negative.

We have  $f'(x) = 40x^4 - 20x^3 = 20x^3(2x - 1)$ .

The distinct real roots of  $f'(x)$  are 0 and  $\frac{1}{2}$ .

For  $x < 0$ ,  $20x^3$  is negative and so is  $2x - 1$ , so that  $f'(x)$  is positive. If  $x_1 < x_2 \leq 0$  then, by the theorem applied to the interval  $[x_1, x_2]$ ,  $f(x_1) < f(x_2)$ . Hence  $f(x)$  is monotonically increasing for  $x \leq 0$ .

For  $0 < x < \frac{1}{2}$ ,  $20x^3$  is positive and  $2x - 1$  is negative, so that  $f'(x)$  is negative. Hence  $f(x)$  is monotonically decreasing for  $0 \leq x \leq \frac{1}{2}$ .

For  $x > \frac{1}{2}$  each of the factors of  $f'(x)$  is positive, so that  $f'(x)$  is also. Hence, as above,  $f(x)$  is monotonically increasing for  $x \geq \frac{1}{2}$ .

## Exercises

- 1 Find the domains in which each of the following is monotonically increasing or monotonically decreasing:

a)  $x^3 - 6x^2 + 11$

f)  $2x^3 - 9x^2 - 60$

b)  $3x^4 - 8x^3 + 6x^2 - 1$

g)  $6x^5 - 15x^4 + 10x^3 + 30$

c)  $x^4 - 4x^3 + 1$

h)  $x^5 - 5x^4 + 256$

d)  $2x^3 - 9x^2 - 60x - 60$

i)  $x^6 - 6x^5 + 2048$

e)  $8x^6 - 24x^2 + 9$

j)  $24x^5 + 15x^4 - 20x^3 + 1$

- 2 If  $f(x)$  and  $g(x)$  have real coefficients,  $g(a) \neq g(b)$ ,  $g'(x)$  never zero for  $a < x < b$ , then there is an  $x_0$  between  $a$  and  $b$  such that

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f'(x_0)}{g'(x_0)}$$

[Hint: Apply Rolle's theorem to  $f(x)[g(a) - g(b)] + g(x)[f(b) - f(a)] + f(a)g(b) - f(b)g(a)$ . The mean-value theorem is a special case with  $g(x) = x$ .]

- \*3 If  $f(x)$  and  $g(x)$  have real coefficients and  $g(x)$  is never zero in  $[a, b]$ , then there is an  $x_0$  between  $a$  and  $b$  such that

$$\frac{f(b) - f(a)}{g(b) - g(a)} = \frac{g(x_0)f'(x_0) - f(x_0)g'(x_0)}{g^2(x_0)} (b-a)$$

[Hint: Let

$$\varphi(x) \equiv f(x) - \frac{f(a)}{g(a)} g(x) + \left[ \frac{f(a)}{g(a)} - \frac{f(b)}{g(b)} \right] \frac{x-a}{b-a} g(x)$$

and apply the theorem of §6 to  $g(x) = \varphi(x) - g'(x)\varphi(x)$ . The theorem of the mean is a special case with  $g(x) = 1$ .]

- 4 If  $f(x)$  has real coefficients,  $r$  is real and  $f'(r)$  positive, then there is an interval  $[a, b]$  such that  $a < r < b$  and  $f(x)$  is monotonically increasing in  $[a, b]$ . Similarly, if  $f'(r)$  is negative, then  $f(x)$  is monotonically decreasing in  $[a, b]$ .
- \*5 If  $f(x)$  has real coefficients and is nowhere zero in  $[a, b]$ , then there is a positive number  $M$  such that either  $f(x) > M$  for every  $x$  in the interval or  $f(x) < -M$  for every  $x$  in the interval. [Hint: By considering the possible real roots of  $f'(x)$ , divide  $[a, b]$  into smaller intervals in each of which  $f(x)$  is monotonic.]

8. **Graphs** One way to locate the real roots of  $f(x)$  is to observe where the graph of  $f(x)$  meets the  $x$  axis. For a close approximation to the roots a fairly accurate graph may be necessary. A rough one



suffices for determining merely the number of real roots. However, a graph should always be sufficiently accurate so as not to yield false or misleading information concerning the matters under consideration.

Suppose, for example, the polynomial is  $f(x) \equiv 8x^5 - 5x^4 + \frac{1}{32}$ .

If we proceed to plot the graph in the usual way, we first make a table of values of  $x$  and the corresponding values of  $f(x)$ . Doing this for  $x = -2, -1, 0, 1, 2$ , we obtain

$x$	$-2$	$-1$	$0$	$\frac{1}{32}$	$2$
$y$	$-1075\frac{1}{32}$	$-415\frac{1}{32}$	$\frac{1}{32}$	$97\frac{1}{32}$	$5633\frac{1}{32}$

If we plot these points and draw a smooth curve through them, we obtain the graph in Fig. 1.

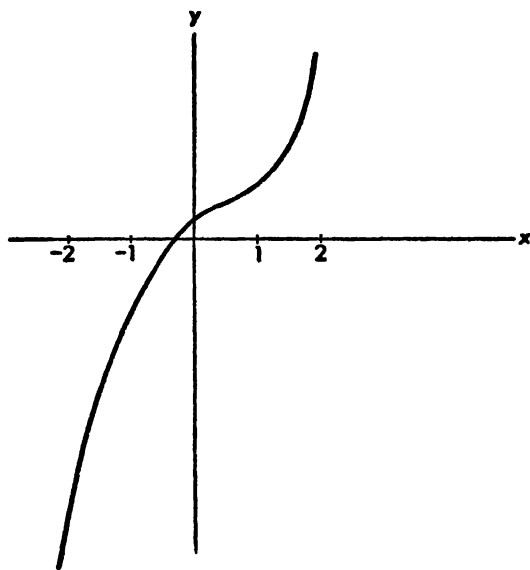


Fig. 1

This graph, however, is misleading. We note that  $f(\frac{1}{32}) = -\frac{1}{32}$ , so that a truer picture is given by Fig. 2.

From Fig. 1 we would have said that  $f(x)$  has only one real root but from Fig. 2 we realize that it has three real roots.

How can one be sure that a graph is not misleading? Plotting points, no matter how many, is not sufficient, since the behavior of the graph between the plotted points will always be in doubt unless one brings in other considerations.

If one is interested, as we shall be, only in the number and approximate location of the real roots, a sufficiently accurate graph can be obtained by determining those sections along which  $y$  increases as  $x$  increases and those sections along which  $y$  decreases as  $x$  increases. This tells us where the graph rises and where it falls as we move from left to right. It also gives us the "turning points"

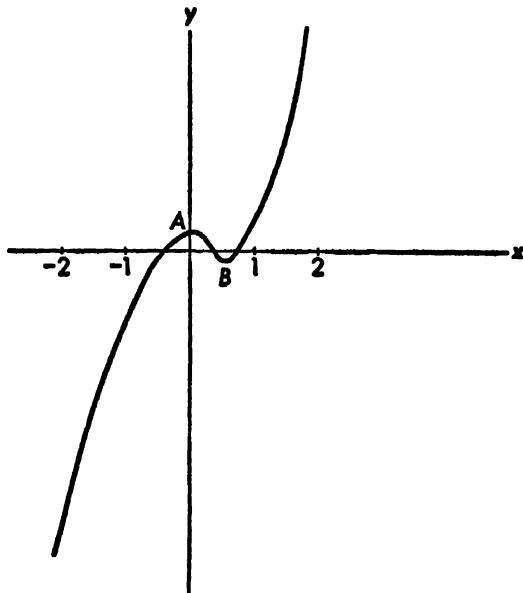


Fig. 2

of the graph, that is, the "maximum" and "minimum" points such as  $A$  and  $B$  in Fig. 2.

To obtain this information concerning a graph, we have only to proceed as in the example of §7. We saw there, for instance, that  $8x^5 - 5x^4 + \frac{1}{32}$  is monotonically increasing for  $x \leq 0$  and for  $x \geq \frac{1}{2}$  and monotonically decreasing for  $0 \leq x \leq \frac{1}{2}$ . If we plot the points for which  $x = 0$  and  $x = \frac{1}{2}$ , and perhaps a few other points, we see that Fig. 2 does give a fairly true picture.

### Exercises

Plot the graphs of the polynomials in ex. 1, §7.

## THEOREMS OF BUDAN AND STURM

**1. Introduction** We continue the discussion of polynomials with real coefficients begun in Ch. 5. We shall be interested in ways of determining the number and approximate location of the real roots.

By means of Sturm's theorem we can determine the number of roots of a polynomial in any interval, provided each root is counted once regardless of its multiplicity. If we wish to take into account the multiplicities of the roots, Budan's theorem may be used. In general, Budan's theorem does not give as precise a result as Sturm's, as we shall see. However, it has the advantage of usually not requiring as much computation. The use of both theorems will frequently give more information than either one by itself.

**2. Variations in sign** Let  $a_0, a_1, \dots, a_{n-1}, a_n$  be a sequence of real numbers,  $n \geq 0$ . Disregard any zeros which may appear. We define the number of variations in sign in the sequence, denoted by  $V[a_0, a_1, \dots, a_{n-1}, a_n]$ , as the number of times a (non-zero) number follows a (non-zero) number of opposite sign.

For example,  $V[2, \sqrt{2}, 0, -1, 0, -4, 6, 0, 0, -1, 0] = 3$ , since there is one variation in sign in  $\sqrt{2}, 0, -1$  and one in  $-4, 6$ , and one in  $6, 0, 0, -1$ .

Also,  $V[0, 0, 1] = 0$ .

**3. Budan sequence** Let

$$(1) \quad f_0(x), f_1(x), \dots, f_p(x), \quad p \geq 1,$$

be a sequence of polynomials with real coefficients and  $[a, b]$  a given interval.

We call (1) a Budan sequence [for  $f_0(x)$ ] in  $[a, b]$  if

(a)  $f_p(x)$  has the same sign for every value of  $x$  in  $[a, b]$ .

- (b) for every  $i$ ,  $0 \leq i \leq p-1$ , and every value of  $x$  between  $a$  and  $b$ ,  $f'_i(x)$  and  $f_{i+1}(x)$  either both vanish or both have the same signs
- (c) if  $a < r \leq b$  and  $f_0(r) = f_1(r) = \cdots = f_{p-1}(r) = 0$ ,  $f_p(r) \neq 0$ , for  $i = 1, 2, \dots, p$ , then  $r$  is a root of  $f_0(x)$  of multiplicity  $i$ .

For any non-constant  $f_0(x)$  and any  $[a, b]$  a Budan sequence exists. For if  $f_0(x)$  is of degree  $n > 0$  then the  $n$ th derivative of  $f_0(x)$  is a non-zero constant (ex. 3, §1, Ch. 4). Hence  $f_0(x), f'_0(x), \dots, f_0^{(n)}(x)$  is surely a Budan sequence in every interval since condition (c) is satisfied by virtue of theorem 1, §2, Ch. 4. But for a given  $f_0(x)$  and a given interval there may be other Budan sequences. For instance, if  $f_0^{(p)}(x)$  is any one of the derivatives of  $f_0(x)$  which has no root in  $[a, b]$  then  $f_0(x), f'_0(x), \dots, f_0^{(p)}(x)$  is a Budan sequence in  $[a, b]$ .

For example, if  $f_0(x) \equiv x^6 - x^4 + x^2 + 3x + 1$ , then

$$\begin{aligned} f'_0(x) &\equiv 6x^5 - 4x^3 + 2x + 3 \\ f''_0(x) &\equiv 30x^4 - 12x^2 + 2 \end{aligned}$$

Since  $f''_0(x) = 0$  is satisfied only by imaginary values of  $x^2$ ,  $f''_0(x)$  is never zero when  $x$  is real. Hence, by the location principle,  $f''_0(x)$  has the same sign for every real value of  $x$ . Thus,  $f_0(x), f'_0(x), f''_0(x)$  is a Budan sequence in every interval.

However, for  $f_0(x) \equiv 5x^6 - 3x^5 - 60x^2 + 60x + 1$  in  $[-1, 1]$ , not until  $f_0^{(5)}(x)$  do we obtain a derivative which does not vanish anywhere in the interval. Thus, the simplest Budan sequence we can get by this method is  $f_0(x), f'_0(x), \dots, f_0^{(5)}(x)$ . However, in this example, as in some others, the following observation permits us to obtain a simpler Budan sequence.

Suppose

$$\begin{aligned} f'_0(x) &\equiv g_1(x)f_1(x) \\ f'_1(x) &\equiv g_2(x)f_2(x) \\ &\vdots \\ f'_i(x) &\equiv g_{i+1}(x)f_{i+1}(x) \\ &\vdots \end{aligned}$$

where  $g_1(x), g_2(x), \dots$  are polynomials with real coefficients which are positive for every value of  $x$  in the domain  $a < x \leq b$  (for example, they may be positive constants). Then, we say,  $f_0(x), f_1(x), \dots, f_p(x)$ , for any  $p \geq 1$ , satisfies conditions (b) and (c) for a Budan sequence in  $[a, b]$ .

That condition (b) is satisfied is obvious since  $g_{n+1}(x) > 0$  for  $a < x \leq b$ .

To consider (c), we show first that for  $k \geq 1$   $f_0^{(k)}(x)$  has the form

$$f_0^{(k)}(x) \equiv g_1(x)g_2(x) \cdots g_k(x)f_k(x) + A_{k-1}(x)f_{k-1}(x) + \cdots + A_1(x)f_1(x)$$

where  $A_{k-1}(x), \dots, A_1(x)$  are polynomials with real coefficients.

For  $k = 1$  this is true (in a vacuous way, i.e., with no  $A$ 's). Proceeding by mathematical induction, suppose it true for  $f_0^{(k)}$ . Then, by differentiation,

$$\begin{aligned} f_0^{(k+1)} &\equiv (g_1 \cdots g_k)f_k' + (g_1 \cdots g_k)'f_k + A_{k-1}f_{k-1}' + A_{k-1}'f_{k-1} \\ &\quad + \cdots + A_1f_1' + A_1'f_1 \\ &\equiv g_1 \cdots g_k g_{k+1}f_k + (g_1 \cdots g_k)'f_k + A_{k-1}g_k f_k + A_{k-1}'f_{k-1} \\ &\quad + \cdots + A_1 g_1 f_1 + A_1'f_1 \\ &\equiv g_1 \cdots g_{k+1}f_{k+1} + B_k f_k + \cdots + B_1 f_1 \end{aligned}$$

which establishes the desired result for  $f_0^{(k+1)}$ .

Now, to consider (c), suppose  $f_0(r) = f_1(r) = \cdots = f_{i-1}(r) = 0$ ,  $f_i(r) \neq 0$ , where  $a < r \leq b$ . Then, for  $k = 1, 2, \dots, i-1$ ,  $f_0^{(k)}(r) = g_1(r) \cdots g_k(r)f_k(r) + A_{k-1}(r)f_{k-1}(r) + \cdots + A_1(r)f_1(r) = 0$  and  $f_0^{(i)}(r) = g_1(r) \cdots g_i(r)f_i(r) + A_{i-1}(r)f_{i-1}(r) + \cdots + A_1(r)f_1(r) = g_1(r) \cdots g_i(r)f_i(r) \neq 0$

Thus, by theorem 1, §2, Ch. 1,  $r$  is a root of  $f_0(x)$  of multiplicity  $i$ .

Applying this observation to the example above,

$$\begin{aligned} f_0(x) &= 5x^6 - 3x^5 - 60x^2 + 60x + 1 \\ f_0'(x) &\equiv 15(1-x^4)(1-2x) \end{aligned}$$

Since  $15(1-x^4)$  is positive throughout  $[-1, 1]$ , we may take  $f_1(x) = 1-2x$ . Then for  $f_1(x)$  we may take  $f_1'(x) \equiv -2$ . Thus,  $f_0(x), f_1(x), f_1'(x)$  is a Budan sequence for  $f_0(x)$  in  $[-1, 1]$ .

**4. Budan's theorem** Let  $(1)$  be a Budan sequence for  $f_0(x)$  in  $[a, b]$ . Denote  $V[f_0(x), \dots, f_p(x)]$  for  $x = a$  and  $x = b$  by  $V_a$  and  $V_b$  respectively. Let  $N$  be the number of roots of  $f_0(x)$  in the domain  $a < x \leq b$ , each counted as often as its multiplicity. Then:

## THEOREM

$N = V_a - V_b - 2q$  where  $q$  is a non-negative integer.

Before proving the theorem we illustrate its use with one of the examples of §3. We saw that for  $f_0(x) \equiv x^6 - x^4 + x^2 + 3x + 1$ , the sequence  $f_0(x)$ ,  $f_1(x) \equiv 6x^5 - 4x^3 + 2x + 3$ ,  $f_2(x) \equiv 30x^4 - 12x^2 + 2$  is a Budan sequence in every interval. For the domain  $-2 < x \leq 0$  we have

$$\begin{aligned} N &= V_{-2} - V_0 - 2q = V[f_0(-2), f_1(-2), f_2(-2)] - V[f_0(0), \\ &\quad f_1(0), f_2(0)] - 2q \\ &= V[+, -, +] - V[+, +, +] - 2q = 2 - 0 - 2q = 2 - 2q \end{aligned}$$

Since  $N \geq 0$ , the only possible values of  $q$  are 0 and 1. Thus,  $N$  is 2 or 0.

For  $-1 < x \leq 0$ ,  $N = V_{-1} - V_0 - 2q = 1 - 0 - 2q = 1 - 2q$ . The only possible value for  $q$  in this case is 0, so that  $N = 1$ .

Thus,  $f_0(x)$  has one root between  $-1$  and  $0$  and, therefore, also one between  $-2$  and  $-1$ .

We prove the theorem by mathematical induction on  $p$ .

Let  $p = 1$  in (1). Then either  $f_1(x) > 0$  everywhere in  $[a, b]$  or  $f_1(x) < 0$  everywhere in  $[a, b]$ . But  $-f_0(x)$ ,  $-f_1(x)$  is a Budan sequence for  $-f_0(x)$  in  $[a, b]$ , and  $-f_0(x)$  has the same roots with the same multiplicities as  $f_0(x)$ . Also, for every  $x$ ,  $V[f_0(x), f_1(x)] = V[-f_0(x), -f_1(x)]$ . Thus, if we prove the theorem when  $f_1(x) > 0$  it will apply to  $-f_0(x)$ ,  $-f_1(x)$  when  $f_1(x) < 0$ , and will establish the theorem in the latter case.

We suppose, therefore, that  $f_1(x) > 0$  in  $[a, b]$ .

By condition (b),  $f'_0(x) > 0$  for  $a < x < b$ . Hence  $f_0(x)$  is monotonically increasing in  $[a, b]$  (§7, Ch. 5). Therefore,  $f_0(x)$  does not have two distinct roots in  $a \leq x \leq b$ .

Since  $f'_0(x) \neq 0$  in  $a < x < b$ ,  $f_0(x)$  does not have a multiple root between  $a$  and  $b$  (theorem 1, §2, Ch. 4). By condition (c),  $f_0(x)$  does not have a multiple root at  $x = b$ .

Thus,  $N$  is 0 or 1.

If  $f_0(a) \geq 0$  then  $f_0(x) > 0$  for  $a < x \leq b$ . Hence  $N = 0$ ,  $V_a = 0$ ,  $V_b = 0$ .

If  $f_0(a) < 0$  and  $f_0(b) < 0$  then  $f_0(x) < f_0(b) < 0$  for  $a < x < b$ . Hence  $N = 0$ ,  $V_a = 1$ ,  $V_b = 1$ .

If  $f_0(a) < 0$  and  $f_0(b) \geq 0$  then  $N = 1$ ,  $V_a = 1$ ,  $V_b = 0$ .

In each of these cases  $N = V_a - V_b$ . Thus, the theorem is established for  $p = 1$ .

Suppose the desired result established when  $p = k \geq 1$ . Let  $p = k + 1$  in (1). As before, we may and do suppose that  $f_{k+1}(x) > 0$  in  $[a, b]$ .

Since  $f'_k(x)$  has the sign of  $f_{k+1}(x)$  for  $a < x < b$ , therefore  $f_k(x) \neq 0$ .

We consider several cases:

*Case 1*  $f_k(x)$  does not vanish anywhere in  $[a, b]$ .

Then  $f_0(x), f_1(x), \dots, f_k(x)$  is a Budan sequence for  $f_0(x)$  in  $[a, b]$ . Hence, by the hypothesis of the induction,

$$N = V[f_0(a), \dots, f_k(a)] - V[f_0(b), \dots, f_k(b)] - 2q$$

By the location principle,  $f_k(a)$  and  $f_k(b)$  have the same signs, for otherwise  $f_k(x)$  would vanish somewhere in  $[a, b]$ . Also,  $f_{k+1}(a)$  and  $f_{k+1}(b)$  have the same signs. Hence  $V[f_k(a), f_{k+1}(a)] = V[f_k(b), f_{k+1}(b)]$ .

Thus,

$$\begin{aligned} N &= V[f_0(a), \dots, f_k(a)] + V[f_k(a), f_{k+1}(a)] - V[f_0(b), \dots, f_k(b)] \\ &\quad - V[f_k(b), f_{k+1}(b)] - 2q \\ &= V[f_0(a), \dots, f_k(a), f_{k+1}(a)] - V[f_0(b), \dots, f_k(b), f_{k+1}(b)] - 2q \\ &= V_a - V_b - 2q \end{aligned}$$

*Case 2*  $f_k(x)$  vanishes at  $x = a$  and nowhere else in  $[a, b]$ .

Suppose  $a$  is a root of  $f_k(x)$  of multiplicity  $\mu$  and  $f_k(x) \equiv (x - a)^\mu g(x)$ .

$g(x)$  does not vanish anywhere in  $[a, b]$ . Hence it has the same sign for every  $x$  in the interval. This sign is the sign of  $f_k(x)$  throughout  $a < x \leq b$ . By (b) this is also the sign of  $f'_{k-1}(x)$  throughout  $a < x < b$ . It follows that

$$(2) \quad f_0(x), \dots, f_{k-1}(x), g(x)$$

satisfies conditions (a), (b), (c) and, therefore, is a Budan sequence for  $f_0(x)$  in  $[a, b]$ .

By the hypothesis of the induction applied to (2),

$$(3) \quad N = V[f_0(a), \dots, f_{k-1}(a), g(a)] - V[f_0(b), \dots, f_{k-1}(b), g(b)] - 2q.$$

Since  $f_{k+1}(x) > 0$  for  $a \leq x \leq b$ , therefore  $f'_k(x) > 0$  for every  $x$  between  $a$  and  $b$ . Hence  $f_k(x)$  is monotonically increasing in  $[a, b]$ . Therefore  $f_k(x) > f_k(a) = 0$  for  $a < x \leq b$ . Thus,  $f_k(b) > 0$ ,  $g(a) > 0$ ,  $g(b) > 0$ . Consequently,

$$\begin{aligned} V[f_0(a), \dots, f_{k-1}(a), g(a)] &= V[f_0(a), \dots, f_{k-1}(a), 0, g(a)] \\ &= V[f_0(a), \dots, f_{k-1}(a), f_k(a), \\ &\quad f_{k+1}(a)] = V_a \\ V[f_0(b), \dots, f_{k-1}(b), g(b)] &= V[f_0(b), \dots, f_{k-1}(b), g(b), f_{k+1}(b)] \\ &= V[f_0(b), \dots, f_{k-1}(b), f_k(b), \\ &\quad f_{k+1}(b)] = V_b \end{aligned}$$

$$\text{Thus, } N = V_a - V_b - 2q$$

**Case 3**  $f_k(x)$  vanishes at  $x = b$  and nowhere else in  $[a, b]$ .

Suppose  $b$  is a root of  $f_k(x)$  of multiplicity  $\mu$  and  $f_k(x) \equiv (b - x)^\mu g(x)$ . Then  $g(x)$  has constant sign in  $a \leq x \leq b$ , which is the sign of  $f_k(x)$  throughout  $a \leq x < b$ . This is also the sign of  $f'_{k-1}(x)$  throughout  $a < x < b$ . Thus, (2) satisfies conditions (a) and (b) for a Budan sequence.

Suppose, first, that not all of  $f_0(b), \dots, f_{k-1}(b)$  vanish and that  $f_k(b)$  is the last one which is non-zero. Then (2) is a Budan sequence and  $N$  is given by (3).

As in case 2,  $f_k(x)$  is monotonically increasing in  $[a, b]$  so that  $f_k(x) < f_k(b) = 0$  for  $a \leq x < b$ . Thus,  $f_k(a) < 0$ ,  $g(a) < 0$ ,  $g(b) < 0$ . Consequently,

$$\begin{aligned} V[f_0(a), \dots, f_{k-1}(a), g(a)] &= V[f_0(a), \dots, f_{k-1}(a), f_k(a)] \\ &= V[f_0(a), \dots, f_k(a), f_{k+1}(a)] - 1 \\ &= V_a - 1 \\ V[f_0(b), \dots, f_{k-1}(b), g(b)] &= V[f_0(b), \dots, f_k(b)] + V[f_k(b), g(b)] \\ &= V[f_0(b), \dots, f_k(b)] \\ &\quad + V[f_k(b), g(b), f_{k+1}(b)] - 1 \end{aligned}$$

If  $f_k(b) < 0$  then  $V[f_k(b), g(b), f_{k+1}(b)] = 1 = V[f_k(b), f_k(b), f_{k+1}(b)]$ .

If  $f_k(b) > 0$  then  $V[f_k(b), g(b), f_{k+1}(b)] = 2$  and  $V[f_k(b), f_k(b), f_{k+1}(b)] = 0$ .

In either case

$$\begin{aligned} V[f_0(b), \dots, f_{k-1}(b), g(b)] &= V[f_0(b), \dots, f_k(b)] + V[f_k(b), \\ &\quad f_k(b), f_{k+1}(b)] + 2q' - 1 \end{aligned}$$



where  $q'$  is 0 or 1

$$= V_b + 2q' - 1$$

Hence

$$N = (V_a - 1) - (V_b + 2q' - 1) - 2q = V_a - V_b - 2q''$$

where  $q'' \geq 0$ .

Suppose, however, that all of  $f_0(b), \dots, f_{k-1}(b)$  are zero. Then, by condition (c),  $b$  is a root of  $f_0(x)$  of multiplicity  $k+1$ . Also,  $V_b = 0$ .

In this case, since  $f_0(b) = f_1(b) = \dots = f_{k-1}(b) = 0, g(b) \neq 0$ , (2) does not satisfy (c) and, therefore, it is not a Budan sequence. However, as before,  $f_k(x) < 0$  in  $a \leq x < b$ . Since  $f'_{k-1}(x)$  has the same sign as  $f_k(x)$  in  $a < x < b$ ,  $f_{k-1}(x)$  is monotonically decreasing in  $[a, b]$ . Hence in  $a \leq x < b, f_{k-1}(x) > f_k(b) = 0$ .

Continuing this type of argument, we see that  $f_{k+1}(x), f_k(x), \dots, f_0(x)$  are alternately positive and negative in  $a \leq x < b$ . Thus  $f_0(a), f_1(a), \dots, f_{k+1}(a)$  alternate in sign, so that  $V_a = k+1$ .

Since  $f_0(x) \neq 0$  in  $a < x < b$ , and  $b$  is a root of multiplicity  $k+1$ , therefore  $N = k+1$ . Thus,  $N = V_a - V_b$ .

*Case 4*  $f_k(x)$  does not vanish for any  $x$  between  $a$  and  $b$ .

Let  $a < r < b$ . To each of the intervals  $[a, r]$  and  $[r, b]$  one of the preceding three cases applies. Hence, if  $N'$  is the number of roots of  $f_0(x)$  in  $a < x \leq r$  and  $N''$  the number in  $r < x \leq b$ , then

$$N = N' + N'' = V[f_0(a), \dots, f_{k+1}(a)] - V[f_0(r), \dots, f_{k+1}(r)] \\ - 2q' + V[f_0(r), \dots, f_{k+1}(r)] - V[f_0(b), \dots, f_{k+1}(b)] - 2q'' \\ = V_a - V_b - 2q$$

where  $q = q' + q'' \geq 0$ .

*Case 5*  $f_k(x)$  vanishes for one or more values of  $x$  between  $a$  and  $b$ .

Let  $r_1, \dots, r_n$  be the distinct roots of  $f_k(x)$  between  $a$  and  $b$  so arranged that  $a < r_1 < r_2 < \dots < r_n < b$ . Let  $r_0 = a, r_{n+1} = b$ .

Between any two successive  $r$ 's  $f_k(x)$  does not vanish. Applying case 4 to each of the intervals  $[r_{i-1}, r_i]$  and proceeding as in the proof of case 4, the desired result follows.

Thus, the theorem is established for  $p = k+1$ . By the principle of mathematical induction, the proof is complete.

*Remark* When, as in the illustration above, the Budan sequence is  $f_0(x), f'_0(x), f''_0(x), \dots, f_0^{(p)}(x)$ ,  $V_a$  and  $V_b$  can be obtained quickly by successive synthetic divisions. To obtain  $V_a$ , for example, we

have only to note that, for every  $i$ ,  $f_0^{(i)}(a)$  has the same sign as  $f_0^{(i)}(a)/i!$ , which is the coefficient of  $(x-a)^i$  in the Taylor expansion of  $f_0(x)$  in powers of  $x-a$  (§4, Ch. 4). Thus, to obtain  $V_2$  in the illustration, where  $f_0 \equiv x^6 - x^4 + x^2 + 3x + 1$ ,  $f_1 \equiv f'_0$ ,  $f_2 \equiv f''_0$ ,

$$\begin{array}{r}
 \begin{array}{ccccccc}
 1 & 0 & -1 & 0 & 1 & 3 & 1 \\
 & -2 & & 4 & -6 & 12 & -26 & 46 \\
 \hline
 1 & -2 & & 3 & -6 & 13 & -23 & + \\
 & -2 & & 8 & -22 & 56 & -138 & \\
 \hline
 1 & -4 & & 11 & -28 & 69 & - & \\
 & -2 & & 12 & -46 & 148 & & \\
 \hline
 1 & -6 & & 23 & -74 & + & & 
 \end{array}
 & \begin{array}{l}
 \underline{-2} \\
 [= f_0(-2)] \\
 \\
 \left[ = \frac{f'_0(-2)}{1!} \right] \\
 \left[ = \frac{f''_0(-2)}{2!} \right]
 \end{array}
 \end{array}$$

### Exercises

- 1 If  $V_a - V_b = 1$ , there is exactly one root in the domain  $a < x \leq b$ .
- 2 Determine the numbers of roots in the given intervals:
  - a)  $x^4 - 2x^3 - 4x^2 + 6x + 3 = 0$  in  $[-1, 0]$  and  $[2, 3]$
  - b)  $x^3 - 2x^2 + 3x - 1 = 0$  in  $[1, 2]$  and  $[0, 1]$
  - c)  $x^4 + 12x^3 + 14x^2 + 6x - 3 = 0$  in  $[-1, 0]$  and  $[0, 1]$
  - d)  $4x^6 - 8x^5 + 15x^4 + 32x^3 + 12x^2 - 32x + 4 = 0$  in  $[0, 1]$  and  $[-2, -1]$
  - e)  $2x^5 - 5x^3 - 5x^2 + 10x - 4 = 0$  in  $[-3, -1]$  and  $[-1, 0]$
  - f)  $x^n - 2x^2 - 4x + 8 = 0$ ,  $n \geq 3$ , in  $[1, 2]$  and  $[-1, 0]$
  - g)  $x^4 + 8x^3 + ax^2 + 2ax + a = 0$ ,  $a > 0$ , in  $[-1, 1]$
- 3 Determine the number of roots of  $x^3 + 3ax + 1 = 0$  between 0 and 1 for all real values of  $a$ .
- 4 Determine the number of roots of  $x^3 + 3ax^2 + 3a^2x + b = 0$  between  $-a$  and  $a$  if  $a$  and  $b$  are real and  $a > 0$ .
- 5 If  $f(x)$  has real coefficients, and the number of roots in  $a < x \leq b$  is  $V_a - V_b - 2q$ , where  $q \geq 0$ , and if  $a < c < b$ , then the number of roots in  $a < x \leq c$  is  $V_a - V_c - 2q'$  where  $0 \leq q' \leq q$ , and the number in  $c < x \leq b$  is  $V_c - V_b - 2q''$  where  $0 \leq q'' \leq q$ .
- 6 Prove:  $V[b_0, b_1, \dots, b_n]$  is even if  $b_0$  and  $b_n$  have the same signs and odd if  $b_0$  and  $b_n$  have opposite signs. Using this, deduce the location principle from Budan's theorem.

### 5. Roots exceeding a given number

#### THEOREM

If  $a$  is a given real number and (1) is a Budan sequence for  $f_0(x)$  in  $[a, b]$  for every  $b > a$ , then the number of roots of  $f_0(x)$  which exceed  $a$ ,



Suppose  $b$  is fixed and we seek the number of roots of  $f_0(x)$  less than  $b$ . Construct a sequence (1) which is a Budan sequence in  $[a, b]$  for every  $a < b$ . Choose  $M$  as above but so great that  $M > -b$ . Then all the roots of  $f_0(x)$  less than  $b$  lie in the domain  $-M < x \leq b$ , and the number of such roots is  $N = V_{-M} - V_b - 2q$ . As before,  $V_{-M}$  can be found without knowing the value of  $M$ , since the sign of  $f_1(-M)$  is the sign of the leading term in  $f_1(x)$  for negative values of  $x$ . We can determine easily whether  $b$  is a root of  $f_0(x)$  and what its multiplicity is. From this and  $N$  we can obtain information concerning the number of roots less than  $b$ .

Another way to find the number of roots less than  $b$  is to find the number of roots of  $g(x) \equiv f_0(-x)$  which exceed  $-b$ . For if  $r < b$  is a root of  $f_0(x)$ , then  $-r > -b$  is a root of  $g(x)$  of the same multiplicity, and conversely.

If we are interested only in the number of real roots of  $f_0(x)$ , we can construct (1) as a Budan sequence in every interval. Then, if we choose  $M$  as above, every real root of  $f_0(x)$  lies in the domain  $-M < x \leq M$ , and the number of such roots is  $V_{-M} - V_M - 2q$ . As before,  $V_M = 0$  and we can find  $V_{-M}$  without knowing  $M$ .

*Example* Find the number of positive and negative roots of  $f(x) \equiv x^5 - x^4 + x^3 + 8x^2 + 2x - 2$ .

$$\begin{aligned}\text{We have } f'(x) &\equiv 5x^4 - 4x^3 + 3x^2 + 16x + 2 \\ f''(x) &\equiv 20x^3 - 12x^2 + 6x + 16 \\ f'''(x) &\equiv 60x^2 - 24x + 6\end{aligned}$$

Since  $f'''(x)$  has no real roots, it has the same sign for every real value of  $x$ . Hence,  $f(x), f'(x), f''(x), f'''(x)$  is a Budan sequence in every interval.

$$\begin{aligned}V_M &= V[+, +, +, +] = 0, & V_0 &= V[-2, 2, 16, 6] = 1, \\ V_{-M} &= V[-, +, -, +] = 3\end{aligned}$$

The number of positive roots is  $V_0 - V_{-M} - 2q = 1 - 2q$ . The only possible value of  $q$  is 0. Hence the number of positive roots is 1.

The number of negative roots is  $V_{-M} - V_0 - 2q = 2 - 2q$ . The only possible values of  $q$  are 0 and 1. Hence the number of negative roots is 2 or 0. Since  $f(0)$  is negative and  $f(-1)$  is positive, there is at least one negative root. Therefore, the number of negative roots is 2.

By Descartes' rule alone, applied to  $f(x)$  and  $f(-x)$ , we would have found that the number of positive roots of  $f(x)$  is 1 or 3 and the number of negative roots 0 or 2.

### Exercises

- 1 If there is exactly one variation in sign in the sequence formed by the coefficients of  $f(x)$ , then  $f(x)$  has exactly one positive root.
- 2 Find the number of roots satisfying the given conditions:
  - a)  $x^3 - 6x^2 + 4x - 5 = 0$ ; greater than 2, greater than -3
  - b)  $x^4 + 3x^2 - 4x + 2 = 0$ ; greater than 1, greater than -2
  - c)  $4x^4 - 8x^3 - x^2 - 5x + 7 = 0$ ; less than 1, less than -2
  - d)  $2x^3 - 4x^2 + 5x - 1 = 0$ ; less than  $\frac{1}{2}$ , less than 0
  - e)  $2x^3 - 12x^2 + 27x - 21 = 0$ ; greater than 2, less than -2
  - f)  $5x^6 - 18x^5 + 5x^3 + 15x^2 - 7x - 10 = 0$ ; greater than 3
  - g)  $x^4 - x^3 + 6x^2 - a = 0$  where  $a > 6$ ; greater than 1
  - h)  $x^3 + ax^2 + [(a^2/3) - 3]x + 3a = 0$  where  $a \leq 0$ ; greater than  $a$
  - i)  $x^4 + ax^3 - a^2x^2 + (2 - 5a^3)x + 4a^4 = 0$  where  $a > 0$ ; greater than  $a$
- 3 Determine to the extent possible the numbers of positive and negative roots:
  - a)  $x^6 + 3x^4 + 2x^2 + 4 = 0$
  - b)  $x^8 + 5x^4 + 4x - 10 = 0$
  - c)  $2x^3 - 4x^2 + 5x - 1 = 0$
  - d)  $5x^4 - 2x^3 + 5x^2 + 4x - 1 = 0$
  - e)  $x^3 - 3x + 1 = 0$
  - f)  $2x^6 + 11x^4 - 3x^3 - x - 4 = 0$
  - g)  $x^5 - 2x^3 + 14x - 1 = 0$
  - h)  $x^4 - 3x^2 + 4x - 1 = 0$
  - i)  $2x^4 - 3x^3 + 4x^2 - x + 5 = 0$
  - j)  $x^4 - x^3 + 6x^2 - a = 0, a > 0$
  - k)  $x^{2n+1} + ax + b = 0, n \geq 1, a > 0, b$  real
  - l)  $(x+1)^n + (x-1)^n - 3 = 0, n \geq 1$
- 4 If  $f(x) \neq 0$  has real coefficients and all its roots are real and non-zero, then the number of positive roots equals the number of variations in sign in the sequence formed by the coefficients.
- 5 Let (1) above be a Budan sequence for  $f_a(x)$  in every interval. Suppose  $f_a(x)$  of degree  $n$  with leading coefficient  $a_n$ . Show that the number of real roots of  $f_a(x)$  is  $\frac{1}{2}[(-1)^na_0, (-1)^{n-1}a_1, \dots, (-1)^na_n] - 2q$  where  $q \geq 0$ .
- 6 Suppose  $f(x)$  of degree  $n$  with real coefficients,  $a < b, f(b) \neq 0$ .
  - a) Show that the expression obtained by multiplying  $f(a+bx)/(1+x)$  by  $(1+x)^n$  represents a polynomial  $g(x)$  of degree  $n$  with real coefficients.

- b) Show that the number of positive roots of  $g(x)$ , if each root be counted as often as its multiplicity, equals the number of roots of  $f(x)$  between  $a$  and  $b$ .
- c) Deduce from Descartes' rule a method for determining the number of roots of  $f(x)$  between  $a$  and  $b$ .
- (This criterion is due to Jacobi.)

### 6. Sturm sequence Let

$$(4) \quad f_0(x), f_1(x), \dots, f_p(x), p \geq 1,$$

be a sequence of polynomials with real coefficients, none vanishing identically.

We call (4) a Sturm sequence [for  $f_0(x)$ ] in  $[a, b]$  if

- (a)  $f_p(x)$  has the same sign for every value of  $x$  in  $[a, b]$
- (b) for  $1 \leq i \leq p-1$ , if  $r$  is in  $[a, b]$  and  $f_i(r) = 0$ , then  $f_{i-1}(r)f_{i+1}(r) < 0$
- (c) for every value of  $x$  between  $a$  and  $b$ ,  $f_1(x)$  and  $f'_0(x)$  either both vanish or both have the same signs
- (d)  $f_0(x)$  has no multiple root in  $[a, b]$ .

If a non-constant polynomial  $f_0(x)$  has no multiple root in  $[a, b]$ , it is always possible to construct a Sturm sequence for it in  $[a, b]$ , as follows:

Let  $f'_0(x) \equiv g_1(x)f_1(x)$  where  $g_1(x) > 0$  in  $[a, b]$  (for example,  $g_1(x) \equiv 1$ ). Since  $f_0(x)$  is not a constant,  $f'_0(x) \not\equiv 0$ . Hence,  $f_1(x) \not\equiv 0$ . Write the division algorithm (§6, Ch. 2) in the form

$$f_0(x) \equiv q_1(x)f_1(x) - g_2(x)f_2(x)$$

where  $g_2(x) > 0$  in  $[a, b]$ .

If  $f_2(x) \not\equiv 0$  then, in the same way,

$$f_1(x) \equiv q_2(x)f_2(x) - g_3(x)f_3(x)$$

where  $g_3(x) > 0$  in  $[a, b]$ .

If we continue the process, the degrees of the remainders keep diminishing. Since the degree of a polynomial cannot be negative, the process cannot continue indefinitely. Therefore, we must eventually obtain the zero polynomial as a remainder. If  $f_p(x)$  is the last non-zero  $f_i(x)$ , we have

$$\begin{aligned} \text{and} \quad & f'_0(x) \equiv g_1(x)f_1(x) \\ & f_0(x) \equiv q_1(x)f_1(x) - g_2(x)f_2(x) \\ & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ & f_{i-1}(x) \equiv q_i(x)f_i(x) - g_{i+1}(x)f_{i+1}(x) \\ & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ & f_{p-2}(x) \equiv q_{p-1}(x)f_{p-1}(x) - g_p(x)f_p(x) \\ & f_{p-1}(x) \equiv q_p(x)f_p(x) \end{aligned}$$

where  $g_1(x), \dots, g_p(x)$  are positive throughout  $[a, b]$ .

We say that  $f_0(x), f_1(x), \dots, f_r(x)$  is a Sturm sequence in  $[a, b]$ .

Conditions (c) and (d) are obviously satisfied. To investigate the others, note first that no two consecutive polynomials in the sequence can vanish at a point  $r$  in  $[a, b]$ . For if  $f_i(r) = f_{i-1}(r) = 0$ , then  $f_{i-1}(r) = 0$  and, working up the sequence,  $f_{i-2}(r) = \dots = f_1(r) = f_0(r) = 0$ . Thus,  $f'_0(r) = 0$ ,  $f_0(r) = 0$ , which is impossible since  $f_0(x)$  has no multiple root in  $[a, b]$  (theorem 2, §2, Ch. 4).

It follows that  $f_p(r) \neq 0$  for  $r$  in  $[a, b]$ ; for if  $f_p(r) = 0$  then also  $f_{p-1}(r) = 0$ , and we have just seen that this is impossible. Thus, by the location principle,  $f_p(x)$  has the same sign throughout  $[a, b]$ .

Also, if  $f_i(r) = 0$  where  $1 \leq i \leq p-1$  and  $r$  is in  $[a, b]$ , then  $f_{i-1}(r) = -g_{i+1}(r)f_{i+1}(r)$ . Since  $f_{i+1}(r) \neq 0$  and  $g_{i+1}(r) > 0$ ,  $f_{i-1}(r)$  and  $f_{i+1}(r)$  have opposite signs. Hence condition (c) is satisfied, and the proof that  $f_0(x), \dots, f_p(x)$  is a Sturm sequence in  $[a, b]$  is complete.

This algorithm for obtaining a Sturm sequence is similar to the Euclidean algorithm of §8, Ch 2. We remark that if  $f_p(x)$  does not vanish anywhere in  $[a, b]$  it follows, without making it a hypothesis, that  $f_0(x)$  has no multiple root in  $[a, b]$ . For if  $r$  is a multiple root of  $f_0(x)$  in  $[a, b]$ , then  $f'_0(r) = 0$ ; hence also  $f_1(r) = 0$ . Working down the algorithm, we see  $f_2(r) = \cdots = f_{p-1}(r) = f_p(r) = 0$ , which contradicts the assumption concerning  $f_p(x)$ .

**Example** Find a Sturm sequence for  $f_0(x) \equiv 12x^6 - 6x^4 + 9x^2 + 8$  in  $[-2, 2]$ .

Let  $f_1(x) \equiv \frac{1}{6}f'_0(x) \equiv 12x^5 - 4x^3 + 3x$ . Then

$$f_0(x) \equiv 4f_1(x) - 2(x^2 + 1)(x^2 - 4)$$

Since  $2(x^2 + 1) > 0$  in  $[-2, 2]$ , we take  $f_2(x) \equiv x^2 - 4$ .

Since  $f_1(x) \equiv (12x^3 + 44x)f_2(x) - 179(-x)$ , we take  $f_3(x) \equiv -x$ . Then  $f_3(x) \equiv (-x)f_3(x) - 4$ , so that  $f_4(x) \equiv 1$ .

By the remark above,  $f_0(x), f_1(x), f_2(x), f_3(x), f_4(x)$  is a Sturm sequence in  $[-2, 2]$ .

**7. Sturm's theorem** Let (4) be a Sturm sequence for  $f_0(x)$  in  $[a, b]$ . Denote  $V[f_0(x), f_1(x), \dots, f_p(x)]$  for  $x = a$  and  $x = b$  by  $V_a$  and  $V_b$  respectively. Let  $N$  be the number of roots of  $f_0(x)$  in the domain  $a < x \leq b$ .

### THEOREM

$$N = V_a - V_b.$$

*Proof:* We proceed by mathematical induction on  $p$ .

For  $p = 1$  the proof is exactly the same as the proof of Budan's theorem when  $p = 1$  (§4). (In fact, for  $p = 1$  a Sturm sequence is also a Budan sequence.)

Suppose the theorem established for  $p = k \geq 1$ . Let  $p = k + 1$ .

*Case 1*  $f_k(x)$  does not vanish anywhere in  $[a, b]$ .

The proof is similar to the proof of case 1 of Budan's theorem.

*Case 2*  $f_k(x)$  vanishes at  $x = a$  and nowhere else in  $[a, b]$ .

Suppose  $a$  is a root of  $f_k(x)$  of multiplicity  $\mu$  and

$$f_k(x) \equiv (x - a)^\mu g(x).$$

$g(x)$  does not vanish anywhere in  $[a, b]$ . Hence it has the same sign for every  $x$  in the interval. This sign is the sign of  $f_k(x)$  throughout  $a < x \leq b$ . It follows immediately that

$$(5) \quad f_0(x), \dots, f_{k-1}(x), g(x)$$

satisfies conditions (a), (c), (d) for a Sturm sequence in  $[a, b]$ . Also, condition (b) is obviously satisfied if  $1 \leq i \leq k - 2$ . To see if (b) is satisfied when  $i = k - 1$ , if  $k - 1 \geq 1$ , suppose  $f_{k-1}(r) = 0$  and  $r$  is in  $[a, b]$ . Then  $f_{k-2}(r)f_k(r) < 0$ . Hence  $r \neq a$ , so that  $g(r)$  and  $f_k(r)$  have the same signs. Therefore,  $f_{k-2}(r)g(r) < 0$ .

Thus, (5) is a Sturm sequence in  $[a, b]$ .

By the hypothesis of the induction applied to (5),

$$N = V[f_0(a), \dots, f_{k-1}(a), g(a)] - V[f_0(b), \dots, f_{k-1}(b), g(b)]$$



$g(a)$  and  $g(b)$  have the same sign, that of  $f_k(b)$ . Hence

$$N = V[f_0(a), \dots, f_{k-1}(a), f_k(b)] - V[f_0(b), \dots, f_{k-1}(b), f_k(b)]$$

Since  $f_k(a) = 0$  and  $f_{k-1}(a), f_{k+1}(a)$  have opposite signs,

$$\begin{aligned} V_a &= V[f_0(a), \dots, f_{k-1}(a), f_k(a), f_{k+1}(a)] \\ &= V[f_0(a), \dots, f_{k-1}(a)] + V[f_{k-1}(a), f_k(a), f_{k+1}(a)] \\ &= V[f_0(a), \dots, f_{k-1}(a)] + 1 \\ &= V[f_0(a), \dots, f_{k-1}(a)] + V[f_{k-1}(a), f_k(b)] - V[f_{k-1}(a), f_k(b)] \\ &\quad + 1 \\ &= V[f_0(a), \dots, f_{k-1}(a), f_k(b)] - V[f_{k-1}(a), f_k(b)] + 1 \\ V_b &= V[f_0(b), \dots, f_k(b), f_{k+1}(b)] \\ &= V[f_0(b), \dots, f_i(b)] + V[f_i(b), f_{k+1}(b)] \end{aligned}$$

Thus,

$$\begin{aligned} N &= (V_a - 1 + V[f_{k-1}(a), f_k(b)]) - (V_b - V[f_k(b), f_{k+1}(b)]) \\ &= V_a - V_b - 1 + V[f_{k-1}(a), f_i(b)] + V[f_i(b), f_{k+1}(b)] \end{aligned}$$

The sign of  $f_{k-1}(a)$  is opposite that of  $f_{k-1}(b)$  which, in turn, is the same as that of  $f_{k+1}(b)$ . Hence,  $f_{k-1}(a)$  has the sign of  $-f_{k+1}(b)$ . Thus,

$$N = V_a - V_b - 1 + V[-f_{k+1}(b), f_k(b)] + V[f_i(b), f_{k+1}(b)]$$

If  $f_k(b)$  and  $f_{i+1}(b)$  have the same signs, then  $V[-f_{k+1}(b), f_k(b)] = 1$  and  $V[f_i(b), f_{i+1}(b)] = 0$

If  $f_k(b)$  and  $f_{i+1}(b)$  have opposite signs, then  $V[-f_{k+1}(b), f_i(b)] = 0$  and  $V[f_k(b), f_{i+1}(b)] = 1$ .

In either case,  $N = V_a - V_b$ .

**Case 3**  $f_k(x)$  vanishes at  $x = b$  and nowhere else in  $[a, b]$ .

The proof is the same as in case 2 except that we let  $f_k(x) \equiv (b-x)^p g(x)$  in order that throughout the domain  $a \leq x < b$  the sign of  $g(x)$  shall be the same as that of  $f_k(x)$ .

**Case 4**  $f_k(x)$  does not vanish for any  $x$  between  $a$  and  $b$ .

The proof is similar to the proof of case 4 of Budan's theorem.

**Case 5**  $f_k(x)$  vanishes for one or more values of  $x$  between  $a$  and  $b$ .

The proof is similar to the proof of case 5 of Budan's theorem.

Thus, the theorem is established for  $p = k + 1$ . By the principle of mathematical induction, the proof is complete.

**Example** Find the number of roots of  $f_0(x) \equiv 12x^5 - 6x^4 + 9x^3 + 8$  in  $[-2, 2]$ .

We saw in §6 that in  $[-2, 2]$   $f_0(x)$ ,  $f_1(x) \equiv 12x^5 - 4x^3 + 3x$ ,  $f_2(x) \equiv x^2 - 4$ ,  $f_3(x) \equiv -x$ ,  $f_4(x) \equiv 1$  is a Sturm sequence.

$$V_{-2} = V[+, -, 0, +, +] = 2, \quad V_2 = V[+, +, 0, -, +] = 2$$

The number of roots in  $-2 < x \leq 2$  is  $V_{-2} - V_2 = 0$ . Since  $f_0(-2) \neq 0$ , there is no root in the interval  $-2 \leq x \leq 2$ .

**Remark** Sturm's theorem cannot be applied to  $f(x)$  if  $f(x)$  has a multiple root in  $[a, b]$ , for no Sturm sequence for  $f(x)$  in  $[a, b]$  can then exist. But if  $D(x)$  is a highest common factor of  $f(x)$  and  $f'(x)$ , and  $f(x) \equiv D(x)f_0(x)$ , then  $f_0(x)$  has exactly the same roots as  $f(x)$  but each root is simple (theorem 6, §2, Ch. 4). We can apply Sturm's theorem to  $f_0(x)$  and thus find the number of roots of  $f(x)$  in  $a < x \leq b$ , each counted once regardless of its multiplicity.

### Exercises

1 Find the number of roots in each of the given intervals:

- $x^3 - 3x + 4 = 0$ ;  $[0, 1]$  and  $[1, 2]$
- $x^4 - 4x^3 + 2 = 0$ ;  $[1, 2]$  and  $[3, 4]$
- $12x^5 - 6x^4 + 9x^3 + 8 = 0$ ;  $[-1, 1]$  and  $[-5, 5]$
- $x^5 - 5x + 8 = 0$ ;  $[0, 3]$  and  $[-2, 0]$
- $x^5 - 8x^2 + 21x + 40 = 0$ ;  $[-2, 0]$  and  $[0, 1]$
- $x^4 - 7x^2 + 2x + 2 = 0$ ;  $[-3, -\frac{1}{2}]$  and  $[-\frac{1}{2}, 0]$
- $x^4 + x^3 - 2x^2 - 3x - 3 = 0$ ;  $[1, 2]$  and  $[-1, 0]$
- $x^5 - 60x^3 - 40x^2 + 270x + 216 = 0$ ;  $[0, 8]$  and  $[-8, 0]$
- $x^{10} - 15x^2 + 40x + 48 = 0$ ;  $[0, 1]$  and  $[-2, 0]$
- $x^5 + 20x^2 - 30x + 48 = 0$ ;  $[-4, -3]$  and  $[1, 2]$
- $x^4 + 12x^3 + 14x^2 + 6x - 3 = 0$ ;  $[0, 1]$  and  $[-1, 0]$
- $2x^5 - 5x^3 - 5x^2 + 10x - 4 = 0$ ;  $[-1, 0]$  and  $[-3, -1]$

2 Show that

- $x^n - n(n-1)x^2 - n(n-2)x + 2(n-1)(n-2) = 0$  has two roots in  $[-1, 1]$  if  $n = 3$  and one if  $n \geq 4$
- $x^n - nx^2 + n - 2 = 0$ ,  $n \geq 3$ , has one root in  $[-1, 0]$  and one root in  $[0, 1]$
- $x^n - nx + 2(1-n) = 0$  has one root in  $[-2, 2]$  if  $n$  is odd and greater than 4, two if  $n$  is even and greater than 3, none if  $n = 3$ , one if  $n = 2$ .

3 Show that

- $x^3 + 3x^2 + 3ax - 2a - 2 = 0$  has one root in  $[-a, a]$  if  $a > 1$
- $x^3 + 3ax^2 + 6a^2x + 2a^3 = 0$  has one root in  $[-a, a]$  if  $a > 0$

- c)  $x^3 + 3ax^2 + 3x + a + 1 - 2a^2 = 0$  has one root in  $[0, a]$  if  $a \geq 1$  and none if  $0 < a < 1$   
 d)  $x^4 + 4x^3 + 6x^2 + 4ax + 4a - 3 = 0$  has one root in  $[0, 1]$  if  $-1 \leq a \leq \frac{3}{4}$  and none for other real values of  $a$ .

**8. Roots exceeding a given number** Let  $M$  be a positive number so chosen that each of the  $f_i(x)$  in (4) has the sign of its leading term whenever  $|x| \geq M$  (§5, Ch. 5). Then  $f_0(x) \neq 0$  when  $|x| \geq M$ .  $V_M$  and  $V_{-M}$  can be found without our knowing the value of  $M$ , since the signs of  $f_i(M)$  and  $f_i(-M)$  are the signs of the leading terms.

Let  $a$  be a given real number and (4) a Sturm sequence for  $f_0(x)$  in  $[a, b]$  for every  $b > a$ . Then, if  $M$  be chosen larger than  $a$ , all the roots of  $f_0(x)$  which exceed  $a$  are in the domain  $a < x \leq M$ . Hence, the number of these roots is  $V_a - V_M$ .

Similarly, if  $b$  is a given real number and (4) is a Sturm sequence for  $f_0(x)$  in  $[a, b]$  for every  $a < b$ , and if  $M$  be chosen larger than  $-b$ , all the roots of  $f_0(x)$  satisfying  $x \leq b$  are in the domain  $-M < x \leq b$ . Hence, the number of such roots is  $V_{-M} - V_b$ .

If (4) is a Sturm sequence for  $f_0(x)$  in every interval, then all the real roots of  $f_0(x)$  are in the domain  $-M < x \leq M$ , and the number of such roots is  $V_{-M} - V_M$ .

*Example* Locate the real roots of  $f_0(x) = x^6 - 6x^2 + 24x - 36$ .

Let  $f_1(x) = \frac{1}{6}f_0'(x) = x^5 - 2x + 4$ . Then  $f_0(x) \equiv xf_1(x) - 4(x^2 - 5x + 9)$ .

Since  $x^2 - 5x + 9$  has no real root, it has the same sign for all real values of  $x$ . Hence, if we take this as  $f_2(x)$ , then  $f_0(x), f_1(x), f_2(x)$  is a Sturm sequence in every interval.

$$V_0 = V[-, +, +] = 1, \quad V_M = V[+, +, +] = 0, \\ V_{-M} = V[+, -, +] = 2$$

Since  $V_0 - V_M = 1$ ,  $V_{-M} - V_0 = 1$ , there is one positive root and one negative root.

Since  $V_1 - V_2 = V[-, +, +] - V[+, +, +] = 1 - 0 = 1$ , the positive root is in  $[1, 2]$ .

Since  $V_{-1} - V_{-2} = V[+, -, +] - V[-, -, +] = 2 - 1 = 1$ , the negative root is in  $[-3, -2]$ .

## Exercises

1 Find the numbers of positive and negative roots:

- |                                     |                                  |
|-------------------------------------|----------------------------------|
| a) $x^3 + 3x^2 - 9x - 67 = 0$       | g) $x^4 - 3x^2 + 4x - 1 = 0$     |
| b) $x^4 + 4x + 6 = 0$               | h) $x^5 - 5x + 8 = 0$            |
| c) $x^4 + 12x - 5 = 0$              | i) $x^4 - 2x^2 - 12x - 8 = 0$    |
| d) $2x^4 - 3x^3 + 4x^2 - x + 5 = 0$ | j) $x^5 - 5x^2 + 10x - 4 = 0$    |
| e) $x^5 + 10x^2 - 3 = 0$            | k) $5x^6 - 30x^2 + 24x - 20 = 0$ |
| f) $x^6 + 2x^3 - 6x - 7 = 0$        | l) $x^5 - 2x^2 - 3x - 2 = 0$     |

2 Locate the real roots between successive integers:

- |                               |                                 |
|-------------------------------|---------------------------------|
| a) $2x^3 - 3x^2 - 4x - 1 = 0$ | c) $2x^4 - 14x^2 + 14x - 7 = 0$ |
| b) $2x^3 - 3x^2 - 6x - 7 = 0$ | f) $x^4 + 4x^3 - 6x + 3 = 0$    |
| c) $x^3 + 3x^2 - 2x - 5 = 0$  | g) $x^5 - x - 1 = 0$            |
| d) $x^3 + 3x^2 - 3x + 2 = 0$  | h) $x^4 - 4x^3 - 4x + 4 = 0$    |

3 Show that:

- $x^4 - 7x^2 + 2x + 2 = 0$  has no root greater than 3.
- $x^5 + 20x^2 - 30x + 12 = 0$  has no root greater than -3.
- The absolute value of every real root of  $x^{10} - 5x^4 + 15x^2 - 3 = 0$  is less than 1.
- $x^4 + 3x^2 - 4x + 2 = 0$  has no root greater than -2.
- One root of  $x^3 - 6x^2 + 4x - 5 = 0$  exceeds -3 and this root also exceeds 2.
- If  $a < 0$ , one root of  $x^3 + ax^2 + [(a^2/3) - 3]x + 3a = 0$  exceeds  $a$ .

4 Find the number of real roots for all real values of  $a$ :

- |                                    |                                     |
|------------------------------------|-------------------------------------|
| a) $x^6 + 3ax^2 + 6ax + 5a = 0$    | d) $x^4 + 4x^3 + 8x^2 + a = 0$      |
| b) $x^6 + 15ax^2 - 12ax + 20a = 0$ | e) $x^5 - 2ax^3 + ax + a^2 + 1 = 0$ |
| c) $ax^5 + 5x - 4 = 0$             |                                     |

- If  $a$  and  $b$  are real, then  $x^3 + 3ax + 2b = 0$  has one real root if  $a^3 + b^2 > 0$  and three real roots if  $a^3 + b^2 \leq 0$ .
- If  $f_0(x)$  is of degree  $n \geq 1$  and  $f_0(x), \dots, f_p(x)$ ,  $p \leq n$ , is a Sturm sequence in every interval, then  $f_0(x)$  has at least  $n - p$  imaginary roots.

## APPROXIMATIONS TO REAL ROOTS

**1. Introduction** Suppose we seek the real roots of a polynomial  $f(x)$  with real coefficients. If  $f(x)$  is linear or quadratic we can obtain exact expressions for the roots in terms of the coefficients. The same is true if  $f(x)$  is cubic or quartic (as we shall see, Ch. 8), but the expressions are not very simple; in fact, it may even be difficult to recognize from the expressions whether any of the roots are real.

For fifth and higher degree polynomials the situation is even worse, since there cannot exist expressions for the roots in terms of the coefficients if the expressions are to involve only radicals and rational operations. (This point is discussed at greater length in §1, Ch. 8). For such polynomials, and even for those of third and fourth degrees, it may be important as a practical matter to be able to approximate to the real roots with any required degree of accuracy.

**2. Graphical approximation** One way to obtain approximate values of the real roots of  $f(x)$  is to graph  $f(x)$  and estimate the abscissas of the points where the graph meets the  $x$  axis. Once the roots have been located approximately by means of a rough graph, it becomes a matter merely of careful plotting to determine them more accurately.

Suppose, for example, we seek to the nearest hundredth the root of  $f(x) = 8x^5 - 5x^4 + \frac{1}{32}$  (whose graph was discussed in §8, Ch. 5) which lies between 0 and  $\frac{1}{2}$ . We could plot very carefully the portion of the graph from  $x = 0$  to  $x = \frac{1}{2}$  on a large sheet of plotting paper, allowing each square to stand for one one-hundredth of a unit, and read off the root to the nearest hundredth.

Obviously, however, in order to do this we may need an imprac-

tically large sheet. It might be simpler first to let each square denote one-tenth of a unit, and thus locate the root to the nearest tenth. For the example above we would find that the root lies between 0.3 and 0.4. Then, allowing each square on the paper to denote one one-hundredth of a unit, we could plot the portion of the graph from  $x = 0.3$  to  $x = 0.4$  and determine the second decimal place in the approximation.

By this method of graphical approximation we can obtain the root with any required degree of accuracy. But it depends upon careful plotting and it is clearly time and space consuming.

### Exercises

Obtain graphically, to the nearest tenth, the real roots of the polynomials in ex. 1, §7, Ch. 5.

**3. Approximation by location principle** Suppose  $f(a)$  and  $f(b)$  have opposite signs. Then, by the location principle, there is a root  $r$  between  $a$  and  $b$ . Suppose  $f(x)$  has no other root between  $a$  and  $b$ .

Arbitrarily choose a number  $c$  between  $a$  and  $b$  as a first approximation to  $r$ . If perchance  $f(c) = 0$ , then we have the desired root. Otherwise,  $f(c)$  has the same sign as  $f(a)$  or the same sign as  $f(b)$ . In the first case,  $r$  is between  $c$  and  $b$ ; in the second case, between  $a$  and  $c$ . In either case, we have narrowed the interval in which the root must lie.

We can now proceed with the smaller interval as we did with the original interval, obtaining a second approximation and narrowing the interval still further. We may continue this process as long as we wish, getting better and better approximations to the root.

If we choose  $c$  at random at each stage, there is no assurance that we shall be able to get as close to the root as we may wish. There are, however, systematic ways of choosing the approximations that will assure, after a sufficient number of steps, an approximation that differs from the root by less than a preassigned amount. There are, in fact, many such systems, although there is no one which is best for all polynomials.

If  $a \neq b$  and  $f(a)$  and  $f(b)$  have the same signs,  $f(x)$  may still have a root between  $a$  and  $b$  but it is impossible, by considering only the signs of  $f(a)$ ,  $f(b)$ , and  $f(c)$ , to determine whether the root lies

between  $a$  and  $c$  or between  $c$  and  $b$ . But if  $D(x)$  is a highest common factor of  $f(x)$  and  $f'(x)$ , and  $f(x) \equiv D(x)g(x)$ , then  $g(x)$  has the same roots as  $f(x)$  but each root is simple (theorem 6, §2, Ch. 4). Then if  $f(x)$  has a unique root between  $a$  and  $b$ ,  $g(a)$  and  $g(b)$  have opposite signs, and the process above can be applied to  $g(x)$ .

**4. Determination of successive decimal places** Suppose we seek a root of  $f(x)$  to within 0.01, the root having already been located between the successive integers  $a$  and  $a + 1$ . We can divide the interval  $[a, a + 1]$  into 100 equal parts by letting  $x$  have the values  $a + 0, a + 0.01, a + 0.02, \dots, a + 0.99, a + 1$ . By determining the signs of  $f(x)$  for each of these values of  $x$ , assuming that  $f(a)$  and  $f(a + 1)$  have opposite signs, we can decide between which successive two of these values of  $x$  the root must lie. We can thus locate the root to within 0.01.

Although this method will locate the root at once with the required accuracy, it has the disadvantage that there may be many values of  $x$  to be tried. It will usually require less computation if we first locate the root between successive tenths, then between successive hundredths, then between successive thousandths, etc.

To illustrate the method, we find to the nearest hundredth the positive root of  $f(x) \equiv 2x^3 + 2x^2 - 12x - 15$ .

Since  $f(2) = -15$ ,  $f(3) = 21$ , the root is between 2 and 3. To locate it between successive tenths, we first try 2.5. Since  $f(2.5) = -1.25$ , the root is between 2.5 and 3.

Since  $f(2.7) = 6.546$ , the root is between 2.5 and 2.7. Since  $f(2.6) = 2.472$ , the root is between 2.5 and 2.6.

To locate the root between successive hundredths, we first try 2.55. Since  $f(2.55) = 0.56775$ , the root is between 2.50 and 2.55.

Since  $f(2.53) = -0.169646$ , the root is between 2.53 and 2.55.

Since  $f(2.54) = 0.197328$ , the root is between 2.53 and 2.54.

Since we seek the root only to the nearest hundredth, we try 2.535. Since  $f(2.535) = 0.01341075$ , the root is between 2.530 and 2.535. Hence, to the nearest hundredth, the root is 2.53.

**5. Horner's method** To make systematic and less cumbersome the computations involved in the method of §4, we may use a method due to Horner.

Suppose we have located the desired root  $r$  between the successive integers  $a$  and  $a + 1$ .

To locate the root between successive tenths, we transform the equation  $f(x) = 0$  into an equation  $g(x) = 0$  whose roots are those of  $f(x)$  each diminished by  $a$ . This can be done by successive synthetic divisions (exs. 3 and 4, §1, Ch. 4). Since  $f(x)$  has a root  $r$  between  $a$  and  $a + 1$ ,  $g(x)$  has a root  $r - a$  which lies between 0 and 1. This root can now be located between successive tenths.

For a value of  $x$  between 0 and 1, the value of  $x^j$ , where  $j$  is a positive integer, is "small" compared with the value of  $x^{j-1}$ . Therefore, in locating the root of  $g(x)$  between 0 and 1, we may, for the purpose of a first approximation, neglect all the terms of  $g(x)$  except those involving the two lowest powers of  $x$ . This gives a reasonable first trial number and may reduce the number of necessary trials.

Suppose we have located the root  $r - a$  of  $g(x)$  between the successive tenths  $b/10$  and  $(b + 1)/10$ . We can now proceed with  $g(x)$  as we did with  $f(x)$ , obtaining a polynomial  $h(x)$  whose roots are those of  $g(x)$  each diminished by  $b/10$ . The polynomial  $h(x)$  has a root between 0 and 0.1. When we have located this root between successive hundredths we shall have located the desired root of  $f(x)$  between successive hundredths.

We can continue this procedure until we obtain as many decimal places as we require.

We illustrate Horner's method by working again the example of §4. We seek the root of  $f(x) \equiv 2x^3 + 2x^2 - 12x - 15$  between 2 and 3.

To reduce the roots by 2, we divide  $f(x)$  and the successive quotients by  $x - 2$ . We have

$$\begin{array}{r|rrrr}
 2 & 2 & -12 & -15 & \\
 & 4 & 12 & 0 & \\
 \hline
 & 2 & 0 & -15 & \\
 & & 4 & 20 & \\
 \hline
 & 2 & 10 & 20 & \\
 & & 4 & & \\
 \hline
 & 2 & 14 & & \\
 & & 2 & & 
 \end{array}$$

The transformed equation is  $g(x) \equiv 2x^2 + 14x + 20 - 15 = 0$ , with a root between 0 and 1.



If we neglect the terms involving  $x^3$  and  $x^2$ , we have  $20x - 15 = 0$ . Hence,  $x = 0.7$  will serve as a first trial number.

We find (by synthetic division)  $g(0.7) = 6.546$ . Since  $g(0) = -15$ , the root is between 0 and 0.7.

Since  $g(0.6) = 2.472$ , the root is between 0 and 0.6. Since  $g(0.5) = -1.25$ , the root of  $g(x)$  is between 0.5 and 0.6.

Thus, the desired root of  $f(x)$  is between 2.5 and 2.6.

To reduce the roots of  $g(x)$  by 0.5, we have

$$\begin{array}{r}
 2 \quad 14 \quad 20 \quad -15 \quad | 0.5 \\
 \quad \quad 1 \quad 7.5 \quad 13.75 \\
 \hline
 2 \quad 15 \quad 27.5 \quad -1.25 \\
 \quad \quad 1 \quad 8 \\
 \hline
 2 \quad 16 \quad 35.5 \\
 \quad \quad 1 \\
 \hline
 2 \quad 17 \\
 \hline
 2
 \end{array}$$

The transformed equation is  $h(x) \equiv 2x^3 + 17x^2 + 35.5x - 1.25 = 0$ , with a root between 0 and 0.1.

Neglecting the  $x^3$  and  $x^2$  terms, we have  $35.5x - 1.25 = 0$ , which gives  $x = 0.03$  as a first trial number.

Since  $h(0.03) = -0.169646$  and  $h(0.1) = g(0.6) = 2.472$ , the root is between 0.03 and 0.10.

Since  $h(0.04) = 0.197328$ , the root is between 0.03 and 0.04.

Thus, the desired root of  $f(x)$  is between 2.53 and 2.54.

To reduce the roots of  $h(x)$  by 0.03, we have

$$\begin{array}{r}
 2 \quad 17 \quad 35.5 \quad -1.25 \quad | 0.03 \\
 \quad \quad 0.06 \quad 0.5118 \quad 1.080354 \\
 \hline
 2 \quad 17.06 \quad 36.0118 \quad -0.169646 \\
 \quad \quad 0.06 \quad 0.5136 \\
 \hline
 2 \quad 17.12 \quad 36.5254 \\
 \quad \quad 0.06 \\
 \hline
 2 \quad 17.18 \\
 \hline
 2
 \end{array}$$

The transformed equation is  $k(x) \equiv 2x^3 + 17.18x^2 + 36.5254x - 0.169646 = 0$ , with a root between 0.00 and 0.01.

Since we seek the root of  $f(x)$  to the nearest hundredth, we have

only to determine whether the root of  $k(x)$  is larger or smaller than 0.005.

Since  $k(0.005) = 0.01341075$  and  $k(0) = -0.169646$ , the root of  $k(x)$  is between 0 and 0.005.

Thus, the desired root of  $f(x)$  is between 2.530 and 2.535. [Actually, the root of  $k(x)$  is between 0.004 and 0.005, so that the root of  $f(x)$  is between 2.534 and 2.535.]

*Remark* When seeking a negative root by Horner's method, it will usually be more convenient, although not necessary, first to transform the given equation into one whose roots are the negatives of those of the given equation (ex. 2, §5, Ch. 3) and then to approximate to the corresponding positive root of the transformed equation.

### Exercises

1 Evaluate to the nearest hundredth:

- The root of  $x^3 - 9x^2 + 19x + 13 = 0$  between 0 and  $-1$
- The negative root of  $2x^3 - 2x^2 - 12x + 15 = 0$
- The smallest real root of  $5x^3 + 18x^2 + 15x - 1 = 0$
- The real cube root of 4
- The real root of  $x^3 + 3x - 5 = 0$
- The positive root of  $x^3 + 3x^2 + 2x - 34 = 0$
- The largest real root of  $2x^4 - 3x^3 - 2x - 2 = 0$
- The smallest positive root of  $x^4 - 7x + 3 = 0$
- The positive fourth root of 6
- The largest real root of  $x^4 + 3x^2 + 6x + 1 = 0$

2 Obtain to the nearest hundredth the real roots of the polynomials in ex. 2, §8, Ch. 6.

3 Obtain to the nearest hundredth the real roots of the polynomials in ex. 1, §7, Ch. 5.

**6. Newton's method** In Newton's method of approximation each approximation is expressed explicitly in terms of the preceding one, and no direct use is made of the location principle.

We first describe the method geometrically.

Suppose  $f(x)$  has a root  $r$  between  $a$  and  $b$ , where  $a < b$ , and that in the interval  $[a, b]$   $f'(x)$  is never zero. Let  $x = c_0$ , any value of  $x$  in the interval, be taken as a first approximation to the root.

The tangent line to the graph of  $f(x)$  at the point for which

$x = c_0$  has slope  $f'(c_0)$ , and an equation for it, in point-slope form, is  $y - f(c_0) = f'(c_0)(x - c_0)$ .

Since  $f'(c_0) \neq 0$ , the tangent line is not parallel to the  $x$  axis. The abscissa of the point where it crosses the  $x$  axis, obtained by letting  $y = 0$  in the equation and solving for  $x$ , is  $c_0 - f(c_0)/f'(c_0)$ . Calling this  $c_1$ , we take it as our second approximation to the root.

Proceeding with  $c_1$  as we did with  $c_0$ , we obtain a third approximation. Continuing thus, we obtain a succession of approximations  $c_0, c_1, \dots, c_n, \dots$  where

$$c_n = c_{n-1} - \frac{f(c_{n-1})}{f'(c_{n-1})} \quad (n = 1, 2, \dots).$$

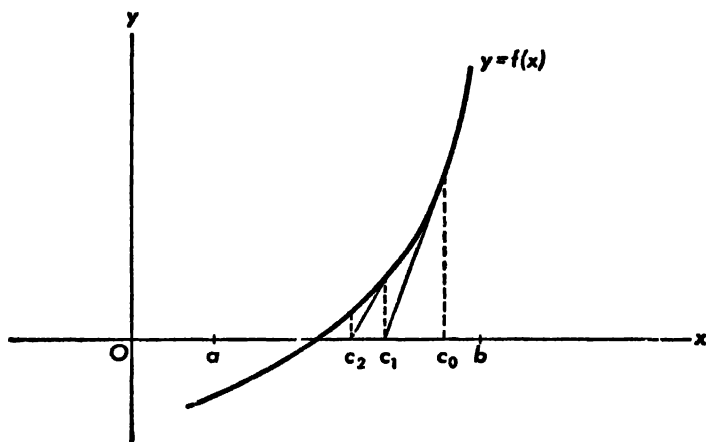


Fig. 1

Disregarding, if we like, this geometric motivation, we may describe Newton's method by saying: let  $c_0$  be any number in the interval  $[a, b]$  and let  $c_n$  for  $n = 1, 2, \dots$  be obtained successively by the preceding formula. These will be taken as the successive approximations to the root  $x = r$ .

It seems intuitively evident, from Fig. 1, that the successive approximations will get closer and closer to the root as  $n$  increases. But there are situations in which this will not be the case. Such a situation is pictured in Fig. 2.

To assure the validity of Newton's method some conditions have to be imposed upon  $f(x)$  and the initial choice for  $c_0$ . We discuss such conditions in the following paragraph.

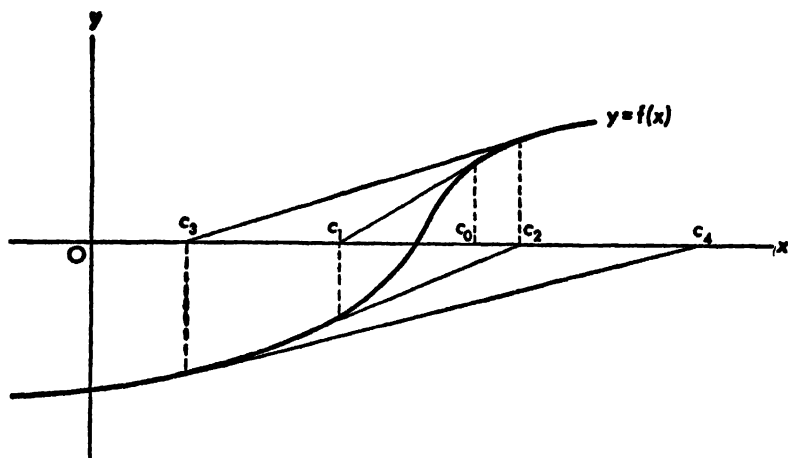


Fig. 2

**7. Validity of Newton's method** Suppose  $f(r) = 0$ ,  $a < r < b$ ,  $f'(x)$  different from zero for every value of  $x$  in  $[a, b]$ .

We show first that if  $c_0$  be properly chosen all the subsequent approximations lie in  $[a, b]$ .

We have

$$c_1 = c_0 - \frac{f(c_0)}{f'(c_0)}$$

so that, since  $f(r) = 0$ ,

$$c_1 - r = \left[ c_0 - \frac{f(c_0)}{f'(c_0)} \right] - \left[ r - \frac{f(r)}{f'(r)} \right]$$

Let  $P(x) \equiv xf'(x) - f(x)$ ,  $Q(x) \equiv f'(x)$ . Then

$$c_1 - r = \frac{P(c_0)}{Q(c_0)} - \frac{P(r)}{Q(r)}$$

$Q(x)$  does not vanish in  $[a, b]$ . Therefore (ex. 3, §7, Ch. 5) if  $c_0 \neq r$ ,

$$\begin{aligned} c_1 - r &= (c_0 - r) \frac{Q(x_0)P'(x_0) - P(x_0)Q'(x_0)}{Q^2(x_0)} \\ &= (c_0 - r) \frac{f(x_0)f''(x_0)}{[f'(x_0)]^2} \end{aligned}$$

where  $x_0$  is between  $c_0$  and  $r$ .

If  $c_0 = r$  this is also true if we take  $x_0 = r$ , since then  $c_1 - r = c_0 - r = 0$ .

Since  $f'(x)$  does not vanish anywhere in  $[a, b]$  there is an  $M > 0$  such that  $|f'(x)| > M$  for every  $x$  in  $[a, b]$  (ex. 5, §7, Ch. 5).

Let  $0 < \lambda < 1$ . Since  $f(x)f''(x)$  vanishes at  $x = r$ , there exists a  $\delta > 0$  such that  $|f(x)f''(x)| < \lambda M^2$  for  $|x - r| < \delta$  (by ex. 21, §4, Ch. 2, taking  $\epsilon = \lambda M^2$ ).

Let  $\alpha$  be a positive number smaller than  $\delta$ ,  $r - a$ , and  $b - r$ . Then, if  $x$  is in  $[r - \alpha, r + \alpha]$ ,

$$r - \alpha \leq x \leq r + \alpha$$

$$-\alpha \leq x - r \leq \alpha$$

$$|x - r| \leq \alpha < \delta$$

and

$$x \leq r + \alpha < r + (b - r) = b$$

$$x \geq r - \alpha > r - (r - a) = a$$

thus,  $x$  is in both  $[a, b]$  and  $|x - r| < \delta$ . For every such  $x$ , therefore,

$$(a) \quad \left| \frac{f(x)f'(x)}{[f'(x)]^2} \right| < \frac{\lambda M^2}{M^2} = \lambda < 1$$

If  $c_0$  is in  $[r - \alpha, r + \alpha]$ , then  $x_0$  is also, and

$$|c_1 - r| < \lambda |c_0 - r| < |c_0 - r| \leq \alpha$$

so that  $c_1$  is also.

It follows in the same way, step by step (actually by mathematical induction), that  $c_0, c_1, \dots$  all lie in  $[r - \alpha, r + \alpha]$ .

Thus, a proper choice for  $c_0$  assures that all the successive approximations lie in  $[a, b]$ . Furthermore, if the interval is such that condition (a) holds throughout the interval (and, as we have seen, one way to assure this is by taking  $[r - \alpha, r + \alpha]$  as the interval), then

$$|c_1 - r| < \lambda |c_0 - r|$$

$$|c_2 - r| < \lambda |c_1 - r| < \lambda^2 |c_0 - r|$$

and, in general,

$$|c_n - r| < \lambda |c_{n-1} - r| < \lambda^n |c_0 - r|$$

Since  $0 < \lambda < 1$ , the successive powers of  $\lambda$  decrease steadily and by taking  $n$  large enough can be made as close to zero as we wish. Hence, if  $n$  be taken large enough,  $|c_n - r|$  will be as small as we please.

*Example* Suppose we seek the positive root of  $2x^3 + 2x^2 - 12x - 15$  (previously obtained by Horner's method in §5).

We first try to obtain a reasonably good first approximation by the location principle.

Since  $f(2.5) = -1.25$ ,  $f(2.6) = 1.472$ , we take as our interval  $[2.5, 2.6]$ .

Since  $f'(x) \equiv 2(3x^2 + 2x - 6)$  has no root in  $[2.5, 2.6]$ , it has the same sign throughout the interval. This sign is positive. Hence,  $f(x)$  is monotonically increasing in the interval. Therefore, for every  $x$  in the interval,

$$-1.25 = f(2.5) \leq f(x) \leq f(2.6) = 1.472$$

so that  $|f(x)| \leq 1.472$ .

Since  $f''(x) \equiv 4(3x + 1)$  is positive throughout the interval,  $f'(x)$  is monotonically increasing in the interval. Hence,  $f'(x) \geq f'(2.5) = 35.5$ .

Also,  $f''(x) \leq f''(2.6) = 35.2$ .

Thus, for every  $x$  in the interval,

$$\left| \frac{f(x)f''(x)}{[f'(x)]^2} \right| \leq \frac{(1.472)(35.2)}{(35.5)^2} = 0.0411^+ = \lambda < 0.042$$

Suppose we choose  $c_0$  so that  $f(c_0)$  is positive. Then  $r < c_0 \leq 2.6$  and

$$c_1 - r = (c_0 - r) \frac{f(x_0)f''(x_0)}{[f'(x_0)]^2}$$

where  $r < x_0 < c_0$ .

Since  $f(x_0)$  and  $f''(x_0)$  are positive,  $c_1 - r$  is positive. Also

$$c_1 - r < (c_0 - r)\lambda < c_0 - r$$

so that  $c_1 < c_0$ .

Hence,  $r < c_1 < c_0$ . Thus,  $c_1$  is in  $[2.5, 2.6]$  and  $f(c_1)$  is positive.

It follows in the same way that  $c_2$  is in  $[2.5, 2.6]$  and  $r < c_2 < c_1 < c_0$ .

Similarly, all the successive approximations lie in the interval  $[2.5, 2.6]$ .

We have

$$\begin{aligned} c_1 - r &< (c_0 - r)\lambda < (0.1)(0.042) = 0.0042 \\ c_2 - r &< (c_0 - r)\lambda^2 < 0.0001764 \end{aligned}$$

## Exercises

- 1 Suppose neither  $f'(x)$  nor  $f''(x)$  vanishes for any  $x$  in  $[a, b]$  and  $|[f(x)f''(x)]/[f'(x)]^2| < \lambda < 1$ . Show that it is possible to choose  $c_0$  in  $[a, b]$  so that  $f(c_0)f''(c_0) > 0$  and if  $c_0$  be so chosen then:
  - a) If  $c_0 < r$  then  $c_0 < c_1 < \cdots < c_n < r$
  - b) If  $c_0 > r$  then  $r > c_n > \cdots > c_1 > c_0$ .
- 2 Make a first approximation to the positive root of  $x^3 - 4x^2 - 16$  by any method and a second by Newton's method. Determine the accuracy of the second approximation.
- 3 Find to two decimal places the largest real root of  $x^3 - x^2 - x - 1 = 0$ .
- 4 Find two approximations to the positive root of  $x^3 - 2x^2 - 20 = 0$  by Newton's method and determine their accuracy.
- 5 Find the positive root of  $x^3 - 2x^2 - 2 = 0$ , making two approximations.
- 6 Find to three decimal places the positive root of  $2x^3 - 3x - 6 = 0$ .
- 7 Locate the real cube root of 7 between successive integers and make a second approximation by Newton's method.
- 8 Find  $\sqrt[3]{3}$  to two decimal places by Newton's method.
- 9 Find the positive root of  $x^3 - 2x - 5 = 0$ .
- 10 Find the root of  $x^3 - 20x + 17 = 0$  between  $-4$  and  $-5$ .  
For practice in the use of Newton's method the exercises following §5 may be worked by this method.

## CUBIC AND QUARTIC EQUATIONS

1. Solvability by radicals If  $f(x) \equiv ax + b$ ,  $a \neq 0$ , then  $f(x)$  has the unique root  $-\frac{b}{a}$ .

If  $f(x) \equiv ax^2 + bx + c$ ,  $a \neq 0$ , the roots are

$$\frac{(-b \pm \sqrt{b^2 - 4ac})}{2a}$$

These are formulas for solving all linear and quadratic equations. They express the roots explicitly in terms of the coefficients.

If  $f(x)$  is of degree  $n > 2$ , it is natural to inquire whether there is a similar formula for the roots of  $f(x)$ . To make the question more precise, note that in the formulas for the roots of linear and quadratic equations the only operations performed upon the coefficients are the rational operations and extractions of roots. That is, these equations are "solvable by radicals."

An equation  $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$  is said to be solvable by radicals if there exists a sequence of numbers  $b_1, b_2, \dots, b_p$  such that every  $b_i$  is either one of the coefficients, or the sum, difference, product, or quotient of  $b_j$  and  $b_k$  where  $j$  and  $k$  are less than  $i$ , or a root (of any index) of a preceding  $b$ , and such that every root of the equation appears in the sequence.

For example, for  $ax^2 + bx + c = 0$ ,  $a \neq 0$ , we have the sequence  $b_1 = a$ ,  $b_2 = b$ ,  $b_3 = c$ ,  $b_4 = b_1/b_1 = 1$ ,  $b_5 = b_1 - b_1 = 0$ ,  $b_6 = b_1b_1 = ac$ ,  $b_7 = b_4 + b_4 = 2$ ,  $b_8 = b_7 + b_7 = 4$ ,  $b_9 = b_6b_8 = 4ac$ ,  $b_{10} = b_2b_2 = b^2$ ,  $b_{11} = b_{10} - b_9 = b^2 - 4ac$ ,  $b_{12} = \sqrt{b_{11}} = \sqrt{b^2 - 4ac}$ ,  $b_{13} = b_5 - b_{12} = -\sqrt{b^2 - 4ac}$ ,  $b_{14} = b_{12} - b_2 = \sqrt{b^2 - 4ac} - b$ ,  $b_{15} = b_{13} - b_2 = -\sqrt{b^2 - 4ac} - b$ ,  $b_{16} = b_1b_7 = 2a$ ,  $b_{17} = b_{14}/b_{16} = (-b + \sqrt{b^2 - 4ac})/2a$ ,  $b_{18} = b_{15}/b_{16} = (-b - \sqrt{b^2 - 4ac})/2a$ . (This is not the only such sequence possible.)



We now ask: Is every equation of degree  $n' > 1$  solvable by radicals?

We shall see in this chapter that for  $n = 3$  and  $n = 4$  the answer is yes. But for  $n > 4$  the answer is no. In fact, even so simple an equation as  $x^5 + 5x - 5 = 0$  is not solvable by radicals. It can be shown that for  $n > 4$  there cannot exist a formula involving only rational operations and root extractions for expressing the roots of every polynomial of degree  $n$  in terms of the coefficients. The proof of this remarkable fact belongs to the Galois theory of equations which we shall not go into. In Ch. 10, however, we shall discuss some matters related to the general question.

2. Cardan's solution of cubic Let the equation be

$$f(x) \equiv x^3 + ax^2 + bx + c = 0$$

where  $a, b, c$  are any complex numbers. For simplicity, we are taking the leading coefficient to be 1.

We first make a transformation to eliminate the second degree term. If the roots of  $f(x)$  are  $x_1, x_2, x_3$ , we seek an equation without a quadratic term whose roots are

$$y_1 = x_1 + \alpha, \quad y_2 = x_2 + \alpha, \quad y_3 = x_3 + \alpha$$

where  $\alpha$  is a constant to be determined.

In the transformed equation the coefficient of the quadratic term is  $-(y_1 + y_2 + y_3) = -(x_1 + x_2 + x_3) - 3\alpha = a - 3$  (§4, Ch. 3). For this to be zero, we desire  $\alpha = a/3$ .

We perform, therefore, the transformation

$$y = x + \frac{a}{3} \quad \text{or} \quad x = y - \frac{a}{3}$$

The transformed equation is

$$\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c = 0$$

or

$$y^3 + py + q = 0$$

where  $p = b - (a^2/3)$ ,  $q = (2a^3 - 9ab + 27c)/27$ .

$y^3 + py + q$  is called the reduced cubic. Its roots are

$$y_1 = x_1 + \frac{a}{3}, \quad y_2 = x_2 + \frac{a}{3}, \quad y_3 = x_3 + \frac{a}{3}$$

To solve the reduced cubic, we use a transformation  $y = z + (\beta/z)$  where  $\beta$  is a constant to be determined. The transformed equation is

$$\left(z + \frac{\beta}{z}\right)^3 + p\left(z + \frac{\beta}{z}\right) + q = 0$$

or 
$$z^3 + \frac{\beta^3}{z^3} + q + (3\beta + p)z + \frac{\beta(3\beta + p)}{z} = 0$$

To eliminate as many terms as possible, it is desirable to have  $3\beta + p = 0$ , or  $\beta = -p/3$ . With this choice for  $\beta$ , the transformation is

$$y = z - \frac{p}{3z}$$

and the transformed equation is

$$z^3 - \frac{p^3}{27z^3} + q = 0$$

or 
$$z^6 + qz^3 - \frac{p^3}{27} = 0$$

This is quadratic in  $z^3$  with the roots

$$z^3 = \frac{1}{2} \left( -q \pm \sqrt{q^2 + \frac{4p^3}{27}} \right)$$

From these expressions for  $z^3$  we shall, in general, obtain six values for  $z$ . For each of the non-zero values of  $z$  we obtain a corresponding value for  $y$  from  $y = z - (p/3z)$ . For each of the values of  $y$  there is a corresponding value for  $x$  from  $x = y - (a/3)$ .

It is clear from the derivation that each of the values of  $x$  thus obtained is a root of  $f(x) = 0$ . Hence, not more than three of the values of  $x$  can be distinct.

Suppose, for example, that the values of  $x$  are 1, 1, 2, 2, 2, 2. What are the roots of  $f(x)$ ? Are they 1, 2, 2 or 1, 1, 2? Evidently we must investigate more closely the manner in which the values of  $x$  are obtained. Since there is no difficulty in the determination

of  $x$  when  $y$  is known, we fix our attention upon the solution of the reduced cubic.

Since  $y$  and  $z$  are related by  $y = z - (p/3z)$ , we are interested only in non-zero values of  $z$ . At least one of the values of  $z^3$  is different from zero unless we simultaneously have

$$-q + \sqrt{q^2 + \frac{4p^3}{27}} = 0, \quad -q - \sqrt{q^2 - \frac{4p^3}{27}} = 0$$

But from these two equalities it follows by addition that  $q = 0$  and, by using  $q = 0$ , that  $p = 0$ . Thus, if both values of  $z^3$  are zero, then  $p = 0$  and  $q = 0$ . In this case the reduced cubic is  $y^3 = 0$  and its roots are 0, 0, 0.

If  $p$  and  $q$  are not both zero, at least one of the values of  $z^3$  is different from zero. Let  $A$  be one of the non-zero values of  $z^3$ . Let  $\sqrt[3]{A}$  be any cube root of  $A$ . If  $\omega$  is either of the imaginary cube roots of 1, i.e.,  $\omega = \frac{1}{2}(-1 \pm i\sqrt{3})$ , then the three cube roots of  $A$  are  $\sqrt[3]{A}$ ,  $\omega \sqrt[3]{A}$ ,  $\omega^2 \sqrt[3]{A}$  (since these are distinct and the cube of each is  $A$ ). We say that these three values of  $z$  in  $y = z - (p/3z)$  give the roots of the reduced cubic, i.e., the roots of the reduced cubic are

$$(1) \quad y_1 = \sqrt[3]{A} - \frac{p}{3\sqrt[3]{A}}, \quad y_2 = \omega \sqrt[3]{A} - \frac{p}{3\omega \sqrt[3]{A}}, \\ y_3 = \omega^2 \sqrt[3]{A} - \frac{p}{3\omega^2 \sqrt[3]{A}}.$$

**3. Verification of the roots** To verify that  $y_1, y_2, y_3$  are the roots of the reduced cubic, we note first that 1,  $\omega$ ,  $\omega^2$ , being the three cube roots of 1, are the roots of  $x^3 - 1 = 0$ . Therefore, their sum  $1 + \omega + \omega^2$  is 0. Also,  $\omega^3 = 1$ ,  $1/\omega = \omega^2$ ,  $1/\omega^2 = \omega$ .

We now have

$$\begin{aligned} y_1 + y_2 + y_3 &= \sqrt[3]{A} (1 + \omega + \omega^2) - \frac{p}{3\sqrt[3]{A}} \left(1 + \frac{1}{\omega} + \frac{1}{\omega^2}\right) \\ &= \sqrt[3]{A} (1 + \omega + \omega^2) - \frac{p}{3\sqrt[3]{A}} (1 + \omega^2 + \omega) \\ &= (1 + \omega + \omega^2) \left(\sqrt[3]{A} - \frac{p}{3\sqrt[3]{A}}\right) \\ &= 0 \end{aligned}$$

$$\begin{aligned}
y_1 y_2 + y_1 y_3 + y_2 y_3 &= (\sqrt[3]{A})^2 (\omega + \omega^2 + \omega^3) \\
&\quad - \frac{p}{3} \left( \omega + \frac{1}{\omega} + \omega^2 + \frac{1}{\omega^2} + \omega + \frac{1}{\omega} \right) \\
&\quad + \frac{p^2}{9(\sqrt[3]{A})^2} \left( \frac{1}{\omega} + \frac{1}{\omega^2} + \frac{1}{\omega^3} \right) \\
&= (\sqrt[3]{A})^2 \omega (1 + \omega + \omega^2) \\
&\quad - \frac{p}{3} (\omega + \omega^2 + \omega^2 + \omega + \omega + \omega^2) \\
&\quad + \frac{p^2}{9(\sqrt[3]{A})^2} (\omega^2 + \omega + 1) \\
&= -p(\omega + \omega^2) \\
&= p \quad \text{since } \omega + \omega^2 = -1 \\
y_1 y_2 y_3 &= \frac{p^2}{9\sqrt[3]{A}} \left( \omega + \frac{1}{\omega} + \frac{1}{\omega^2} \right) - \frac{p\sqrt[3]{A}}{3} \left( \omega^3 + \omega + \frac{1}{\omega} \right) \\
&\quad + \omega^3 (\sqrt[3]{A})^3 - \frac{p^3}{27\omega^3 (\sqrt[3]{A})^3} \\
&= \frac{p^2}{9\sqrt[3]{A}} (\omega + \omega^2 + 1) - \frac{p\sqrt[3]{A}}{3} (1 + \omega + \omega^2) + A - \frac{p^3}{27A} \\
&= A - \frac{p^3}{27A}
\end{aligned}$$

If  $A$  and  $B$  are the roots of the quadratic equation in  $z^3$ , then

$$A + B = -q \quad \text{and} \quad AB = -\frac{p^3}{27}$$

Therefore,  $-\frac{p^3}{27A} = B$  and  $A - \frac{p^3}{27A} = A + B = -q$

Hence,  $y_1 y_2 y_3 = -q$ .

Thus,

$$\begin{aligned}
(y - y_1)(y - y_2)(y - y_3) &= y^3 - (y_1 + y_2 + y_3)y^2 \\
&\quad + (y_1 y_2 + y_1 y_3 + y_2 y_3)y - y_1 y_2 y_3 \\
&= y^3 + py + q
\end{aligned}$$

Hence,  $y_1, y_2, y_3$  are the roots of the reduced cubic.

*Remark* If neither  $A$  nor  $B$  is zero, then, by the argument above, the roots of the reduced cubic are given by (1) and also by

$$\sqrt[3]{B} - \frac{p}{3\sqrt[3]{B}}, \quad \omega \sqrt[3]{B} - \frac{p}{3\omega \sqrt[3]{B}}, \quad \omega^2 \sqrt[3]{B} - \frac{p}{3\omega^2 \sqrt[3]{B}}$$

Therefore, the numbers in the two sets are the same, although perhaps in different order. To find which is equal to which, we must know how the cube roots of  $A$  and  $B$  which appear are related.

Since  $AB = -\frac{p^3}{27}$ , it is possible to choose the cube roots of  $A$  and  $B$  so that their product is  $-\frac{p}{3}$ . If this be done, then  $\sqrt[3]{A} = -\frac{p}{3\sqrt[3]{B}}$  and

$$\begin{aligned} \sqrt[3]{A} - \frac{p}{3\sqrt[3]{A}} &= \sqrt[3]{A} + \sqrt[3]{B} \\ (2) \quad \omega \sqrt[3]{A} - \frac{p}{3\omega \sqrt[3]{A}} &= \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B} \\ \omega^2 \sqrt[3]{A} - \frac{p}{3\omega^2 \sqrt[3]{A}} &= \omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B} \end{aligned}$$

Also

$$\begin{aligned} \sqrt[3]{B} - \frac{p}{3\sqrt[3]{B}} &= \sqrt[3]{B} + \sqrt[3]{A} \\ \omega \sqrt[3]{B} - \frac{p}{3\omega \sqrt[3]{B}} &= \omega \sqrt[3]{B} + \omega^2 \sqrt[3]{A} \\ \omega^2 \sqrt[3]{B} - \frac{p}{3\omega^2 \sqrt[3]{B}} &= \omega^2 \sqrt[3]{B} + \omega \sqrt[3]{A} \end{aligned}$$

Although the formulas (2) were obtained on the assumption that neither  $A$  nor  $B$  is zero, it happens that the right sides give the roots of the reduced cubic even when one or both of  $A$  and  $B$  is zero. For, if  $A$  or  $B$  is zero, then  $AB = -\frac{p^3}{27}$  yields  $p = 0$ . Since  $A$  and  $B$  are the values of  $\frac{1}{2}[-q \pm \sqrt{q^2 + (4p/27)}]$ , and  $p = 0$ , one of  $A$  and  $B$  is zero and the other is  $-q$  (which may also be zero). Thus the right sides in (2) are the cube roots of  $-q$ . But the reduced cubic in this case is  $y^3 + q$  and its roots are also the cube roots of  $-q$ .

4. Example Solve  $x^3 - 6x^2 - 4 = 0$ .

Letting  $y = x + \alpha$ , the sum of the roots of the transformed equation is  $6 + 3\alpha$ . Hence, we choose  $\alpha = -2$ . Therefore,  $x = y + 2$ . This amounts to reducing the roots of the given equa-

tion by 2. The transformed equation can be obtained by replacing  $x$  by  $y + 2$  (§5, Ch. 3) or by repeated synthetic division by  $x - 2$  (exs. 3 and 4, §4, Ch. 4).

By the first method we have

$$(y + 2)^3 - 6(y + 2)^2 - 4 = 0$$

$$y^3 - 12y - 20 = 0$$

By the second method

$$\begin{array}{rrrr} 1 & -6 & 0 & -4 \\ & 2 & -8 & -16 \\ \hline 1 & -4 & -8 & -20 \\ & 2 & -4 & \\ \hline 1 & -2 & -12 & \\ & 2 & & \\ \hline 1 & 0 & & \\ \hline 1 & & & \end{array} \quad \begin{array}{l} 2 \\ 2 \\ 2 \\ 2 \end{array}$$

which gives the same transformed equation.

To solve the cubic in  $y$ , let  $y = z + (\beta/z)$ . The equation becomes

$$\left(z + \frac{\beta}{z}\right)^3 - 12\left(z + \frac{\beta}{z}\right) - 20 = 0$$

$$z^3 + \frac{\beta^3}{z^3} + (3\beta - 12)z + \frac{\beta(3\beta - 12)}{z} - 20 = 0$$

Choose  $\beta$  so that  $3\beta - 12 = 0$ , i.e.,  $\beta = 4$ . Then

$$y = z + \frac{4}{z}$$

and

$$z^3 + \frac{64}{z^3} - 20 = 0$$

$$z^6 - 20z^3 + 64 = 0$$

$$(z^3 - 16)(z^3 - 4) = 0$$

$$z^3 = 4, 16$$

Let  $\sqrt[3]{4}$  be the real cube root. Then  $z = \sqrt[3]{4}, \omega \sqrt[3]{4}, \omega^2 \sqrt[3]{4}$  in  $x = y + 2 = z + (4/z) + 2$  yields the roots of the given equation.

To obtain the roots directly from the formulas of §3, let  $p = -12, q = -20$ . Then

$$A = \frac{1}{2} \left( -q - \sqrt{q^2 + \frac{4p^3}{27}} \right) = \frac{1}{2} (20 - \sqrt{400 - 256}) = 4$$

$$B = \frac{1}{2} \left( -q + \sqrt{q^2 + \frac{4p^3}{27}} \right) = \frac{1}{2} (20 + 12) = 16$$

If  $\sqrt[3]{A} = \sqrt[3]{4}$ , then  $\sqrt[3]{B} = \frac{-p}{3\sqrt[3]{A}} = \frac{4}{\sqrt[3]{4}}$

and the roots are  $2 + \sqrt[3]{A} + \sqrt[3]{B}$ ,  $2 + \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B}$ ,  $2 + \omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B}$ .

### Exercises

#### 1 Solve:

a)  $x^3 + 3x^2 + 9x + 5 = 0$

b)  $x^3 - 6x^2 + 24x - 44 = 0$

c)  $x^3 - 3x + 2 = 0$

d)  $x^3 + 6x^2x - 2a^3 = 0$

e)  $x^3 + 3x^2 - 3x + 2i - 5 = 0$

f)  $x^3 + 3ix + 1 + i = 0$

g)  $y^3 - 3\sqrt[3]{4}y + 4 = 0$

h)  $y^3 + 6iy - 1 - 8i = 0$

i)  $y^3 + 6\omega y - 9i = 0$ ,  $\omega$  an imaginary cube root of 1

j)  $x^3 + 12x - 12 = 0$

k)  $y^3 + 15y + 6 = 0$

l)  $x^3 - 3ix + 1 - i = 0$

m)  $y^3 - 12\omega y - 16 = 0$ ,  $\omega$  an imaginary cube root of 1

n)  $x^3 - 27x - 54 = 0$

o)  $x^3 + 6x - 4i = 0$

2 If  $A$  and  $B$  are any complex numbers,  $\omega$  an imaginary cube root of 1, then  $A + B$ ,  $\omega A + \omega^2 B$ ,  $\omega^2 A + \omega B$  are the roots  $x^3 - 3ABx - (A^3 + B^3) = 0$ .

3 Prove that  $\sqrt[3]{1 + \sqrt{25/27}} + \sqrt[3]{1 - \sqrt{25/27}} = 1$  if the cube roots are real. (Hint: Use ex. 2.)

4 Prove that  $\sqrt[3]{1 + \sqrt{2}} + \sqrt[3]{1 - \sqrt{2}}$ , where the cube roots are real, is irrational. (Hint: Use ex. 2.)

5 Prove that  $\sqrt[3]{\frac{-27 + 10i\sqrt{3}}{9}} + \frac{7}{3\sqrt[3]{\frac{-27 + 10i\sqrt{3}}{9}}}$ , where the cube

root is the same in both parts, is rational.

**5. Discriminant of cubic** If  $f(x)$  is of degree  $n > 1$  and  $x_1, x_2, \dots, x_n$  are the roots, then

$$D = (x_1 - x_2)^2(x_1 - x_3)^2 \cdots (x_1 - x_n)^2(x_2 - x_3)^2 \cdots (x_2 - x_n)^2 \cdots (x_{n-1} - x_n)^2$$

(the product of the squares of all the differences  $x_i - x_j$  for  $i \neq j$ ) is called the discriminant of  $f(x)$ .

Evidently,  $D$  is zero if and only if  $f(x)$  has a multiple root.

If  $f(x) \equiv x^2 + ax + b$ , its discriminant is  $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = a^2 - 4b$ . When  $a$  and  $b$  are real, the sign of  $D$  determines whether the roots  $\frac{1}{2}(-a \pm \sqrt{D})$  are real or imaginary. A similar situation exists for the cubic.

### THEOREM

If  $x^3 + ax^2 + bx + c$  has real coefficients, then:

(a) If  $D > 0$ , all the roots are real and distinct.

(b) If  $D = 0$ , all the roots are real and there is a multiple root.

(c) If  $D < 0$ , there is one real root and two (conjugate) imaginary roots.

*Proof:* Since the coefficients are real, imaginary roots occur in conjugate pairs (§1, Ch. 5). Hence there is at least one real root.

If the other roots are real and no two roots are equal, then  $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 > 0$ .

If the other roots are real and there is a multiple root, then  $D = 0$ .

If the other roots are conjugate imaginaries,  $\alpha + \beta i$  and  $\alpha - \beta i$ , where  $\beta \neq 0$ , then

$$D = (x_1 - \alpha - \beta i)^2(x_1 - \alpha + \beta i)^2(\alpha + \beta i - \alpha + \beta i)^2$$

where  $x_1$  is real

$$= [(x_1 - \alpha)^2 + \beta^2]^2(-4\beta^2) < 0$$

Thus, if  $D > 0$  only the first of these three situations is possible, which proves conclusion (a) of the theorem. Conclusions (b) and (c) follow similarly.



The fact that the sign of the discriminant of a cubic determines the nature of the roots is useful since, as we shall now see, the discriminant can be found without a knowledge of the roots.

### THEOREM

If  $f(x) \equiv x^3 + ax^2 + bx + c$ , and  $g(y) \equiv y^3 + py + q$  is the reduced cubic, then  $f(x)$  and  $g(y)$  have the same discriminants.

*Proof:* If  $x_1, x_2, x_3$  are the roots of  $f(x)$ , then

$$y_1 = x_1 + \frac{a}{3}, \quad y_2 = x_2 + \frac{a}{3}, \quad y_3 = x_3 + \frac{a}{3}$$

are the roots of  $g(y)$ . Therefore,  $x_i - x_j = y_i - y_j$  for  $i \neq j$ , so that the discriminants are equal.

### THEOREM

The discriminant of  $y^3 + py + q$  is  $-4p^3 - 27q^2$ .

*Proof:* The roots are

$$\begin{aligned} y_1 &= \sqrt[3]{A} + \sqrt[3]{B}, & y_2 &= \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B}, \\ y_3 &= \omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B} \end{aligned}$$

where  $\omega = \frac{1}{2}(-1 + i\sqrt{3})$ ,  $A$  and  $B$  are the values of  $\frac{1}{2}[-q \pm \sqrt{q^2 + \frac{4}{27}p^3}]$ , and  $\sqrt[3]{A} \sqrt[3]{B} = -\frac{p}{3}$ .

Thus,

$$\begin{aligned} y_1 - y_2 &= (1 - \omega)\sqrt[3]{A} + (1 - \omega^2)\sqrt[3]{B} \\ &= (1 - \omega)[\sqrt[3]{A} + (1 + \omega)\sqrt[3]{B}] \\ &= (1 - \omega)[\sqrt[3]{A} - \omega^2 \sqrt[3]{B}] \\ y_2 - y_3 &= (\omega - \omega^2)\sqrt[3]{A} + (\omega^2 - \omega)\sqrt[3]{B} \\ &= \omega(1 - \omega)[\sqrt[3]{A} - \sqrt[3]{B}] \\ y_3 - y_1 &= (\omega^2 - 1)\sqrt[3]{A} + (\omega - 1)\sqrt[3]{B} \\ &= (1 - \omega)[(-\omega - 1)\sqrt[3]{A} - \sqrt[3]{B}] \\ &= (1 - \omega)[\omega^2 \sqrt[3]{A} - \sqrt[3]{B}] \\ &= \omega^2(1 - \omega)[\sqrt[3]{A} - \omega \sqrt[3]{B}] \end{aligned}$$

$$\begin{aligned}
(y_1 - y_2)(y_2 - y_3)(y_3 - y_1) &= \omega^3(1 - \omega)^3[\sqrt[3]{A} - \sqrt[3]{B}] \\
&\quad [\sqrt[3]{A} - \omega \sqrt[3]{B}][\sqrt[3]{A} - \omega^2 \sqrt[3]{B}] \\
&= \omega^3(1 - \omega)^3[A - (1 + \omega + \omega^2) \\
&\quad (\sqrt[3]{A})^2 \sqrt[3]{B} + (\omega + \omega^2 + \omega^3) \\
&\quad \sqrt[3]{A} (\sqrt[3]{B})^2 - \omega^3 B] \\
&= (1 - \omega)^3(A - B) \\
&= (1 - 3\omega + 3\omega^2 - \omega^3)(A - B) \\
&= -3(\omega - \omega^2)(A - B) \\
&= -3(1 + 2\omega)(A - B)
\end{aligned}$$

since  $\omega^2 = -1 - \omega$ .

But

$$1 + 2\omega = \pm i\sqrt{3} \quad \text{and} \quad A - B = \pm \sqrt{q^2 + \frac{4p^3}{27}}$$

Hence

$$\begin{aligned}
D &= [(y_1 - y_2)(y_2 - y_3)(y_3 - y_1)]^2 \\
&= \left[ \pm 3i\sqrt{3} \sqrt{q^2 + \frac{4p^3}{27}} \right]^2 \\
&= -(27q^2 + 4p^3)
\end{aligned}$$

### THEOREM

The discriminant of  $x^3 + ax^2 + bx + c$  is  $18abc - 4a^3c + a^2b^2 - 4b^3 - 27c^2$ .

*Proof:* For the reduced cubic,

$$p = b - \frac{a^2}{3}, \quad q = \frac{2a^3 - 9ab + 27c}{27}$$

Therefore,

$$D = -(27q^2 + 4p^3) = -\frac{(2a^3 - 9ab + 27c)^2}{27} - 4\left(b - \frac{a^2}{3}\right)^3$$

Simplifying this gives the stated result.

*Example* Determine the nature of the roots of  $x^3 - 9x + 8$ .

Here  $a = 0$ ,  $b = -9$ ,  $c = 8$ ,  $D = 1188$ . Since the coefficients are real and  $D$  is positive, the roots are all real and unequal. [Actually the roots are  $1, \frac{1}{2}(-1 \pm \sqrt{33})$ .]

## Exercises

1 Determine the nature of the roots of:

a)  $x^3 - 3x^2 - 3x - 2 = 0$

d)  $2x^3 + x^2 + x + 1 = 0$

b)  $x^3 - 2x + 9 = 0$

e)  $x^3 + 5x^2 - 2 = 0$

c)  $2x^3 - 7x + 1 = 0$

2 Determine the number of real roots for real values of  $a$ :

a)  $x^3 - 3x + a = 0$

d)  $x^3 + ax^2 + 4a^2x + a^3 = 0$

b)  $x^3 + ax^2 + 4 = 0$

e)  $x^3 + 3ax + 4 = 0$

c)  $ax^3 - 3x + 4 = 0$

f)  $x^3 + 27x^2 + ax + 18a = 0$

3 Determine  $a$  so that there will be a multiple root:

a)  $x^3 - 27x + a = 0$

b)  $4x^3 + 4ax^2 + a^2x + 24a = 0$

c)  $x^3 - 3a^2x + 2a^3 = 0$

d)  $x^3 + ax^2 + 2ax + a + 1 = 0$

e)  $x^3 + 3ax^2 + (3a^2 - 1)x + a^3 - a = 0$

f)  $x^3 + 3ax^2 + 4a = 0$

g)  $x^3 - 2x^2 - (3a - 1)(a + 1)x + 2a(a + 1)^2 = 0$

6. Cubics with three real roots If we solve  $x^3 - 9x + 8 = 0$  by Cardan's method, we obtain the roots

$$\sqrt[3]{-4 + i\sqrt{11}} + \sqrt[3]{-4 - i\sqrt{11}}, \quad \omega \sqrt[3]{-4 + i\sqrt{11}} + \omega^2 \sqrt[3]{-4 - i\sqrt{11}}, \quad \omega^2 \sqrt[3]{-4 + i\sqrt{11}} + \omega \sqrt[3]{-4 - i\sqrt{11}}$$

where  $\sqrt[3]{-4 + i\sqrt{11}}$  and  $\sqrt[3]{-4 - i\sqrt{11}}$  are chosen so that their product is 3. Actually, as we saw in §5, the equation has three real roots, with  $x = 1$  as an obvious root. From the expressions obtained by Cardan's method, however, it is difficult to see that 1 is a root or even that there are any real roots.

Whenever the cubic has real coefficients and the discriminant is positive, the roots are real and distinct, but Cardan's formulas necessarily involve imaginary quantities. For, considering the reduced cubic  $y^3 + py + q = 0$ , the discriminant is  $D = -27q^2 - 4p^3$  and the roots are

$$\sqrt[3]{A} + \sqrt[3]{B}, \quad \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B}, \quad \omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B}$$

where

$$A = \frac{1}{2} \left( -q + \sqrt{q^2 + \frac{4p^3}{27}} \right) = \frac{1}{2} \left( -q + \sqrt{\frac{-D}{27}} \right) \\ = \frac{1}{2} \left( -q + i \sqrt{\frac{D}{27}} \right) \\ B = \frac{1}{2} \left( -q - i \sqrt{\frac{D}{27}} \right)$$

For practical purposes it is sometimes desirable to express the roots in a form which involves no imaginary quantities. This can be done with the help of the triple angle formula

$$4 \cos^3 \theta - 3 \cos \theta = \cos 3\theta$$

From this we see that  $z = \cos \theta$  is one root of

$$(a) \quad z^3 - \frac{3}{4}z - \frac{\cos 3\theta}{4} = 0.$$

But

$$\begin{aligned} \cos(\theta + 120^\circ) &= \cos \theta \cos 120^\circ - \sin \theta \sin 120^\circ \\ &= -\frac{1}{2} \cos \theta - \frac{1}{2} \sqrt{3} \sin \theta \\ \cos(\theta + 240^\circ) &= \cos \theta \cos 240^\circ - \sin \theta \sin 240^\circ \\ &= -\frac{1}{2} \cos \theta + \frac{1}{2} \sqrt{3} \sin \theta \end{aligned}$$

Hence

$$\begin{aligned} \cos \theta + \cos(\theta + 120^\circ) + \cos(\theta + 240^\circ) &= 0 \\ \cos \theta \cos(\theta + 120^\circ) + \cos \theta \cos(\theta + 240^\circ) \\ + \cos(\theta + 120^\circ) \cos(\theta + 240^\circ) &= -\frac{3}{4}(\cos^2 \theta + \sin^2 \theta) = -\frac{3}{4} \\ \cos \theta \cos(\theta + 120^\circ) \cos(\theta + 240^\circ) &= \frac{1}{4} \cos \theta (\cos^2 \theta - 3 \sin^2 \theta) \\ &= \frac{1}{4} \cos \theta (4 \cos^2 \theta - 3) = \frac{1}{4} \cos 3\theta \end{aligned}$$

Therefore,  $\cos \theta$ ,  $\cos(\theta + 120^\circ)$ ,  $\cos(\theta + 240^\circ)$  are the roots of (a).

If the reduced cubic has a positive discriminant, by choosing a suitable  $\lambda$  and letting  $y = \lambda z$  we transform the equation  $y^3 + py + q = 0$  into one of the form (a). The transformed equation, after dividing by  $\lambda^3$ , is

$$z^3 + \frac{p}{\lambda^2}z + \frac{q}{\lambda^3} = 0$$

Hence, we wish

$$\frac{p}{\lambda^2} = -\frac{3}{4}, \quad \frac{q}{\lambda^3} = -\frac{1}{4} \cos 3\theta$$

Since  $D = -27q^2 - 4p^3$  is positive and  $p$  and  $q$  are real,  $p$  is negative. Hence, a real value for  $\lambda = 2\sqrt{\frac{-p}{3}}$  exists. Using this  $\lambda$ , we seek an angle  $\theta$  such that

$$\cos 3\theta = \frac{3q}{2p} \sqrt{\frac{-3}{p}}$$

$D > 0$  implies  $-4p^3 > 27q^2$ . Hence

$$0 \leq \frac{27q^2}{-4p^3} < 1$$

Therefore

$$\left| \frac{3q}{2p} \sqrt{\frac{-3}{p}} \right| < 1$$

so that an angle  $3\theta$  exists with the desired cosine. Thus,  $\theta$  can be found.

With the  $\lambda$  and  $\theta$  thus determined, the transformed equation has the form (a). Since the roots of (a) are  $\cos \theta$ ,  $\cos (\theta + 120^\circ)$ ,  $\cos (\theta + 240^\circ)$ , the roots of the reduced cubic are  $2\sqrt{\frac{-p}{3}} \cos \theta$ ,  $2\sqrt{\frac{-p}{3}} \cos (\theta + 120^\circ)$ ,  $2\sqrt{\frac{-p}{3}} \cos (\theta + 240^\circ)$ .

*Example* Obtain by the trigonometric method the roots of  $y^3 - 9y + 8 = 0$ .

Here  $\lambda = 2\sqrt{3}$ ,  $\cos 3\theta = -(4/9)\sqrt{3}$ . From trigonometric tables we can find the roots approximately. For,  $\cos 3\theta = -0.76980$ ,  $3\theta = 140^\circ 20' 9''$ ,  $\theta = 46^\circ 46' 43''$ . Hence

$$2\sqrt{\frac{-p}{3}} \cos \theta = 2\sqrt{3} \cos 46^\circ 46' 43'' = 2.3724$$

$$2\sqrt{\frac{-p}{3}} \cos (\theta + 120^\circ) = 2\sqrt{3} \cos 166^\circ 46' 43'' = -3.3722$$

$$2\sqrt{\frac{-p}{3}} \cos (\theta + 240^\circ) = 2\sqrt{3} \cos 286^\circ 46' 43'' = 1.0000$$

### Exercises

Solve by the trigonometric method:

a)  $y^3 - 36y - 72 = 0$

d)  $y^3 - 12y + 12 = 0$

b)  $y^3 - 6y + 4 = 0$

e)  $y^3 - 6y - 2 = 0$

c)  $y^3 - 3y + 1 = 0$

f)  $x^3 + 3x^2 - 3x - 9 = 0$

**7. Ferrari's solution of quartic** Finding the roots of a polynomial and factoring the polynomial into linear factors are equivalent problems (§2, Ch. 3). Ferrari's method for solving a quartic is a special device for obtaining the linear factorization.

Let  $y$  be any constant. Then, if  $f(x) \equiv x^4 + ax^3 + bx^2 + cx + d$ , we may rewrite  $f(x)$  in the form

$$\begin{aligned} f(x) &\equiv (x^2 + \frac{1}{2}ax + \frac{1}{2}y)^2 + bx^2 + cx + d - (\frac{1}{4}a^2x^2 + yx^2 \\ &\quad + \frac{1}{2}ayx + \frac{1}{4}y^2) \\ &\equiv (x^2 + \frac{1}{2}ax + \frac{1}{2}y)^2 + (b - \frac{1}{4}a^2 - y)x^2 + (c - \frac{1}{2}ay)x \\ &\quad + (d - \frac{1}{4}y^2) \end{aligned}$$

We shall choose  $y$  so that  $f(x)$  becomes the difference of two squares, i.e., so that  $(b - \frac{1}{4}a^2 - y)x^2 + (c - \frac{1}{2}ay)x + (d - \frac{1}{4}y^2)$  becomes  $-(\lambda x + \mu)^2 \equiv (i\lambda x + i\mu)^2$ . This will happen if and only if the roots of this quadratic in  $x$  are equal; hence, if and only if the discriminant is zero. Thus, we wish to choose  $y$  so that

$$(c - \frac{1}{2}ay)^2 - 4(b - \frac{1}{4}a^2 - y)(d - \frac{1}{4}y^2) = 0$$

Simplifying this equation, we obtain

$$y^3 - by^2 + (ac - 4d)y + 4bd - a^2d - c^2 = 0$$

This cubic in  $y$  is called the resolvent cubic of  $f(x)$ . It is not necessary to solve the equation completely since all we need is one value for  $y$ .

Having chosen  $y$  as a root of the resolvent cubic, we have

$$\begin{aligned} f(x) &\equiv (x^2 + \frac{1}{2}ax + \frac{1}{2}y)^2 - (\lambda x + \mu)^2 \\ &\quad (\lambda \text{ or } \mu \text{ or both may be zero}) \\ &\equiv (x^2 + \frac{1}{2}ax + \frac{1}{2}y + \lambda x + \mu)(x^2 + \frac{1}{2}ax + \frac{1}{2}y - \lambda x - \mu). \end{aligned}$$

The roots of  $f(x)$  are the roots of the quadratic factors.

We remark that the values of  $\lambda$  and  $\mu$  may depend upon which root of the resolvent cubic we take for  $y$ . The final factorization of  $f(x)$  into linear factors, however, is the same regardless of which value of  $y$  we use (§1, Ch. 3).

**Example** Find the roots of  $f(x) \equiv x^4 + 2x^3 + 4x^2 + 4x + 2$ .

Following Ferrari's method, we have

$$\begin{aligned} f(x) &\equiv (x^2 + x + \frac{1}{2}y)^2 + 4x^2 + 4x + 2 - x^2 - yx^2 - yx - \frac{1}{4}y^2 \\ &\equiv (x^2 + x + \frac{1}{2}y)^2 + (3 - y)x^2 + (4 - y)x + (2 - \frac{1}{4}y^2) \end{aligned}$$

The resolvent cubic is

$$4(3 - y)(2 - \frac{1}{4}y^2) - (4 - y)^2 \equiv y^3 - 4y^2 + 8$$

Obviously, 2 is a root of the cubic. Hence

$$\begin{aligned} f(x) &\equiv (x^2 + x + 1)^2 + x^2 + 2x + 1 \\ &\equiv (x^2 + x + 1)^2 + (x + 1)^2 \\ &\equiv (x^2 + x + 1 + ix + i)(x^2 + x + 1 - ix - i) \end{aligned}$$

The roots of the quadratic factors are  $\frac{1}{2}(-1 - i \pm \sqrt{-4 - 2i})$  and  $\frac{1}{2}(-1 + i \pm \sqrt{-4 + 2i})$ .

### Exercises

1 Solve:

- |  |  |
|--|--|
| a) $x^4 + 2\sqrt{5}x^3 + 5x^2 - 1 = 0$ | m) $x^4 + 4x^3 + 7x^2 + 10x + 3 = 0$                     |
| b) $x^4 + 3x - 2 = 0$                  | n) $x^4 - 3x + 20 = 0$                                   |
| c) $x^4 + 4x^3 + 27 = 0$               | o) $x^4 + 8x + 63 = 0$                                   |
| d) $x^4 - 7x^2 + 2x + 2 = 0$           | p) $x^4 + x^3 + 2x + 6 = 0$                              |
| e) $x^4 + 2x^3 - x^2 + 2x + 1 = 0$     | q) $x^4 + 2x^3 - 4x - 2 = 0$                             |
| f) $x^4 - 2x^3 - 5x^2 + 10x - 3 = 0$   | r) $x^4 + 3ix^2 + \frac{5}{2}(1 + i)x + \frac{9}{2} = 0$ |
| g) $x^4 - 4x^3 + 6x^2 - 11x - 4 = 0$   | s) $16x^4 - 8x^3 - 8x^2 + 2x + 1 = 0$                    |
| h) $x^4 + x^2 + 2ix - 1 = 0$           | t) $x^4 + 2\sqrt{2}/\sqrt{3}x^3 + \frac{3}{4} = 0$       |
| i) $x^4 + 2x^2 - 12ix - 8 = 0$         | u) $x^4 + 12x + 3 = 0$                                   |
| j) $x^4 - 4x^3 + 4x^2 - 4x + 3 = 0$    | v) $x^4 + 4x^3 - 1 = 0$                                  |
| k) $x^4 + 2x^3 + x^2 - 9 = 0$          | w) $x^4 + 4x^3 + 9x^2 + 4x + 4 = 0$                      |
| l) $x^4 + x^2 + 4x - 3 = 0$            |  |

2 The transformation  $y = x + \frac{1}{4}a$ , applied to  $x^4 + ax^3 + bx^2 + cx + d = 0$ , gives a reduced quartic,  $F(y) \equiv y^4 + qy^2 + ry + s = 0$ , containing no term in  $y^3$ . If we attempt to find numbers  $\lambda, \mu, \nu$  such that  $F(y) \equiv (y^2 + \lambda y + \mu)(y^2 - \lambda y + \nu)$  by equating coefficients, we are led to equations from which, by elimination of  $\mu$  and  $\nu$ , we obtain  $\lambda^8 + 2q\lambda^4 + (q^2 - 4s)\lambda^2 - r^2 = 0$ . Letting  $z = \lambda^2$ , we have an auxiliary cubic  $H(z) \equiv z^3 + 2qz^2 + (q^2 - 4s)z - r^2 = 0$ . Let  $G(u)$  be the resolvent cubic for  $F(y)$ . Show that  $G(z + q) \equiv H(z)$ . (Once  $\lambda$  has been determined,  $\mu$  and  $\nu$  can be found. Thus, we have another method for solving a quartic.)

8. Roots of resolvent cubic Let  $g(u) \equiv y^3 - by^2 + (ac - 4d)y + (1bd - a^2d - c^2)$  be the resolvent cubic of  $f(x) \equiv x^4 + ax^3 + bx^2 + cx + d$ .

## THEOREM

If  $x_1, x_2, x_3, x_4$  are the roots of  $f(x)$ , then

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_2x_4, \quad y_3 = x_1x_4 + x_2x_3$$

are the roots of  $g(y)$ .

*Proof:* We have, using the relations between the roots and coefficients (§4, Ch. 3),

$$\begin{aligned} y_1 + y_2 + y_3 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = b \\ y_1y_2 + y_1y_3 + y_2y_3 &= (x_1 + x_2 + x_3 + x_4)(x_1x_2x_3 + x_1x_2x_4 \\ &\quad + x_1x_3x_4 + x_2x_3x_4) - 4x_1x_2x_3x_4 \\ &= ac - 4d \\ y_1y_2y_3 &= -4(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 \\ &\quad + x_3x_4)x_1x_2x_3x_4 \\ &\quad + (x_1 + x_2 + x_3 + x_4)^2x_1x_2x_3x_4 \\ &\quad + (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)^2 \\ &= -4bd + a^2d + c^2 \end{aligned}$$

Thus,

$$(y - y_1)(y - y_2)(y - y_3) \equiv y^3 - by^2 + (ac - 4d)y + (4bd - a^2d - c^2) \equiv g(y)$$

which proves the theorem.

## THEOREM

*The quartic and the resolvent cubic have the same discriminants.*

*Proof:* By the preceding theorem

$$\begin{aligned} (y_1 - y_2)^2(y_2 - y_3)^2(y_3 - y_1)^2 \\ = [(x_1 - x_4)(x_2 - x_3)]^2[(x_1 - x_2)(x_3 - x_4)]^2[(x_1 - x_3)(x_4 - x_2)]^2 \end{aligned}$$

so that the discriminants are the same.

## Exercises

- 1 Prove: A quartic has a multiple root if and only if its resolvent cubic has a multiple root.
- 2 Prove: If a quartic has real coefficients and its resolvent cubic has an imaginary root, then the quartic has an imaginary root.
- 3 Prove: A quartic has a root of multiplicity three or more if and only if all the roots of the resolvent cubic are equal.
- 4 Prove: A quartic has two roots whose sum is zero if and only if the resolvent cubic has two roots whose sum is zero.



- 5 If  $D$  is the discriminant of a quartic with real coefficients and no multiple root, then:
- If the roots are all real or all imaginary  $D > 0$ .
  - If two roots are real and two imaginary,  $D < 0$ .
- 6 Let  $g(y)$  be a given cubic with leading coefficient 1. Prove: There are infinitely many quartics with leading coefficient 1 for which  $g(y)$  is the resolvent cubic. Show that specifying the coefficient of  $x^3$  reduces the number of quartics to either one or two.
- 7 Let  $f_1(x)$  and  $f_2(x')$  be quartics with roots  $x_1, x_2, x_3, x_4$  and  $x'_1, x'_2, x'_3, x'_4$  respectively. Let  $y_1, y_2, y_3$  and  $y'_1, y'_2, y'_3$  be the roots of their resolvent cubics. Prove: If there exists a number  $r$  such that
- $x'_i = rx_i$  ( $i = 1, 2, 3, 4$ ), then there exists a number  $s$  such that  $y'_i = sy_i$  ( $i = 1, 2, 3$ )
  - $x'_i = x_i - r$  ( $i = 1, 2, 3, 4$ ), then there exists a number  $s$  such that  $y'_i = y_i - s$  ( $i = 1, 2, 3$ ).
- 8 Prove: If two quartics have the same resolvent cubics and two common roots, then either they have exactly the same roots or two roots of one are the negatives of two roots of the other.
- 9 Let  $y_1, y_2, y_3$  be the roots of the resolvent cubic of  $x^4 + ax^3 + bx^2 + cx + d$ . Show that it is possible, by choosing the proper square root in each case, to determine  $z_1 = \sqrt{y_1 - b + \frac{1}{4}a^2}$ ,  $z_2 = \sqrt{y_2 - b + \frac{1}{4}a^2}$ ,  $z_3 = \sqrt{y_3 - b + \frac{1}{4}a^2}$  so that  $z_1 z_2 z_3 = \frac{1}{6}a^3 - \frac{1}{2}ab + c$ . Prove then that  $\frac{1}{2}(-z_1 - z_2 - z_3) - \frac{1}{4}a$ ,  $\frac{1}{2}(-z_1 + z_2 + z_3) - \frac{1}{4}a$ ,  $\frac{1}{2}(z_1 - z_2 + z_3) - \frac{1}{4}a$ ,  $\frac{1}{2}(z_1 + z_2 - z_3) - \frac{1}{4}a$  are the roots of the quartic.

## RULER AND COMPASS CONSTRUCTIONS

**1. Definition of constructibility** We shall be concerned with the possibility of carrying out certain geometric constructions using only a straightedge and a pair of compasses.

Let  $S_1$  be a configuration consisting of given points, lines, rays, segments, and circles. (Note: A line extends indefinitely in two directions. A ray is one of the two parts into which a line is divided by a point on it; a ray extends indefinitely in only one direction; the point is called the endpoint. A segment is a portion of a line included between two points of the line; the points are called the endpoints.) We refer to the points, lines, rays, segments, and circles as the figures of the configuration.

Let  $S_2$  be any one of the following.

- (1) A point which is an intersection of two of the figures of  $S_1$
- (2) A segment determined by two points of  $S_1$
- (3) A ray with a point of  $S_1$  as endpoint and containing another point of  $S_1$  or obtained by extending one of the segments of  $S_1$  in one direction
- (4) A line determined by two points of  $S_1$  or obtained by extending a ray or segment of  $S_1$
- (5) A circle with a point of  $S_1$  as center and radius equal to the length of one of the segments of  $S_1$ .

Similarly, let  $S_3$  be obtained in one of these ways from the configuration formed by  $S_1$  and  $S_2$  together.

In general, suppose we have a succession of configurations  $S_1, S_2, \dots, S_n$  each obtained from all the preceding ones in one of the ways described above. If all the figures in a configuration  $S$  are included in  $S_1, S_2, \dots, S_n$ , we say that  $S$  is constructible from  $S_1$  with ruler and compasses (or, for brevity, that  $S$  is constructible from  $S_1$ ).

*Example* Show that the midpoint of a given line segment is constructible with ruler and compasses.

Let  $S_1$  be the given segment  $AB$ . Let  $S_2$  be a circle with center at  $A$  and radius  $AB$ . Let  $S_3$  be a circle with center at  $B$  and radius  $AB$ . Let  $S_4$  be a point of intersection of circles  $S_2$  and  $S_3$  and let  $S_5$  be the other point of intersection. Let  $S_6$  be the segment  $S_4S_5$ . Let  $S_7$  be the point of intersection of  $S_6$  and  $S_1$ .  $S_7$  is the desired point.

### Exercises

In order to have a basis for determination of lengths, we always suppose a unit segment is given.

- 1 Show that the following are ruler and compass constructions:
  - a) On a given ray or line to lay off a segment with a given endpoint and with length equal to that of a given segment
  - b) To construct an angle with a given ray as one side and equal to a given angle (an angle is a figure formed by two rays with a common endpoint)
  - c) To construct a line containing a given point and parallel to a given line not containing the point
  - d) To bisect a given angle.
- \*2 If segments of lengths  $a$  and  $b$  are given, show that it is possible with ruler and compasses to construct a segment of length
  - a)  $a + b$
  - b)  $a - b$  if  $a > b$
  - c)  $ab$
  - d)  $a/b$
  - e)  $\sqrt{a}$
  - f) the absolute value of a root of  $x^2 + ax + b = 0$ , if the roots are real.
- \*3 If configuration  $A$  is constructible from configuration  $B$  and  $B$  is constructible from configuration  $C$ , then  $A$  is constructible from  $C$ .

**2. Criterion for constructibility** To develop a criterion for determining whether a construction can be carried out with ruler and compasses from given figures, we must first discuss what is meant by saying a figure is given. For instance, when we say a line is given, do we mean that every point on the line is known?

We shall simplify the problem by supposing that we are dealing only with plane configurations and that in the plane we have a pair of axes to which all figures can be referred. That is, we suppose

we have the usual rectangular coordinate system. This implies, of course, that we also have a unit segment, the unit of the coordinate system.

From the very nature of the coordinate system, to every real number  $a$  there corresponds a point  $P$  on the  $x$  axis,  $(a, 0)$ , and conversely. When we wish to use geometric language, we may refer to the number  $a$  as the point  $P$ . When we wish to use algebraic language, we may refer to the point  $P$  as the number  $a$ . Thus, " $a$  is given" and " $P$  is given" may be regarded as synonymous.

We agree:

- (a) A point is given if its coordinates are given.
- (b) A segment is given if its endpoints are given.
- (c) A line is given if the numbers  $a, b, c$  in an equation for the line,  $ax + by + c = 0$ , are given.
- (d) A ray is given if its endpoint and the line on which it lies are given.
- (e) A circle is given if the numbers  $a, b, c$  in an equation for the circle,  $x^2 + y^2 + ax + by + c = 0$ , are given.

In each case the numbers will be called the numbers of the figure.

We shall say a configuration is given if the numbers of the figures in the configuration are given. We call these numbers the numbers of the configuration.

We now state:

### THEOREM

*A configuration  $T$  is constructible with ruler and compasses from a configuration  $S$  if and only if the numbers of  $T$  are obtainable from those of  $S$  by rational operations and extractions of real square roots.*

If  $a_1, a_2, \dots$  are complex numbers (a finite number or infinitely many), a number  $r$  is said to be obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots (not necessarily real) if there exists a sequence  $b_1, b_2, \dots, b_p$  such that  $b_p = r$  and each  $b_i$  is one of the  $a$ 's or is a sum, product, difference or quotient of two (not necessarily distinct) preceding  $b$ 's, or is a square root of some preceding  $b$ .

For example, if  $a_1 = -3, a_2 = \frac{1}{2}, r = i\sqrt{3 + \sqrt{\frac{3}{4}}}$ , let  $b_1 = a_1 = -3, b_2 = b_1 - b_1 = 0, b_3 = b_2 - b_1 = 3, b_4 = a_2 = \frac{1}{2}, b_5 =$

$a_2 a_2 = 1/4$ ,  $b_6 = b_5 b_5 = 3/4$ ,  $b_7 = \sqrt{b_6} = \sqrt{3/4}$ ,  $b_8 = b_3 + b_7 = 3 + \sqrt{3/4}$ ,  $b_9 = \sqrt{b_8} = \sqrt{3 + \sqrt{3/4}}$ ,  $b_{10} = b_1/b_3 = -1$ ,  $b_{11} = \sqrt{b_{10}} = i$ ,  $b_{12} = b_{11} b_9 = r$ . (This is not the only such sequence possible.)

If all the  $a$ 's and  $b$ 's are real,  $r$  is said to be obtainable from the  $a$ 's by rational operations and extractions of real square roots.

If there exists such a sequence in which no square roots are necessary,  $r$  is said to be rational in the  $a$ 's.

We can now proceed with the proof of the theorem.

*Part 1* Suppose  $T$  constructible from  $S$  with ruler and compasses.

Let  $S_1, S_2, \dots, S_n$ , with  $S_1 = S$ , be a sequence of configurations such as described in §1, which includes all the figures of  $T$ .

$S_2$  may be a point, segment, i.e., line, or circle. Suppose, for example, it is a point and that it is an intersection of two circles  $x^2 + y^2 + a_1 x + b_1 y + c_1 = 0$  and  $x^2 + y^2 + a_2 x + b_2 y + c_2 = 0$  of  $S_1$ . By subtraction,  $(a_1 - a_2)x + (b_1 - b_2)y + c_1 - c_2 = 0$ . Solving this linear equation simultaneously with one of the two quadratic equations, we see that the coordinates of the points of intersection are obtainable from  $a_1, b_1, c_1, a_2, b_2, c_2$  by rational operations and extractions of square roots. Since the points have real coordinates, only real square roots appear. Thus, in this case, the numbers of  $S_2$  are obtainable from those of  $S_1$  by rational operations and extractions of real square roots.

We leave it to the reader to verify that in every other case the same is true for the numbers of  $S_2$ .

In a similar way, the numbers of  $S_3$  are obtainable from those of  $S_1$  and  $S_2$  by rational operations and extractions of real square roots. It follows (ex. 2 following) that the numbers of  $S_3$  are obtainable from those of  $S_1$  in this way.

Proceeding in this manner, we see that the numbers of each of the  $S_i$ , and therefore those of  $T$ , are obtainable from the numbers of  $S$  in the required way.

*Part 2* To prove the converse, let  $a_1, a_2, \dots, a_m$  be the numbers of  $S$  and  $r_1, r_2, \dots, r_n$  those of  $T$ , and suppose every  $r_i$  is obtainable from the  $a$ 's by rational operations and extractions of real square roots.

Since  $S$  is given, by definition the points  $(a_1, 0), \dots, (a_m, 0)$  are given. We show first that the points  $(r_i, 0)$  are constructible from  $S$ , i.e., from the points  $(a_1, 0), \dots, (a_m, 0)$ .

Let  $r$  denote any one of the  $r_i$ . By hypothesis, there is a sequence  $b_1, b_2, \dots, b_p$  with  $b_p = r$  of the type described above.

Obviously,  $b_1$  is one of the  $a$ 's, so that in a trivial sense  $(b_1, 0)$  is constructible from  $S$ .

To show by mathematical induction that every  $(b_i, 0)$  is constructible from  $S$ , suppose  $(b_1, 0), \dots, (b_{i-1}, 0)$  so constructible. We consider the following cases:

(a)  $b_i$  is one of the  $a$ 's. The desired result follows trivially.

(b)  $b_i = b_j + b_k$  where  $j$  and  $k$  are less than  $i$ .

If  $b_i = 0$  then  $(b_i, 0)$  is the origin, which point we already have. Hence, suppose  $b_i \neq 0$ .

If  $b_j$  or  $b_k$  is zero, there is nothing to be proved since  $j$  and  $k$  are less than  $i$  and the hypothesis of the induction applies.

If  $b_j$  and  $b_k$  are both positive or both negative, then  $|b_i| = |b_j| + |b_k|$ . Hence (ex. 2(a), §1), a segment of length  $|b_i|$  is constructible from segments of lengths  $|b_j|$  and  $|b_k|$ . Since, by the hypothesis of the induction,  $(b_j, 0)$  and  $(b_k, 0)$  are constructible from  $S$ , segments of lengths  $|b_j|$  and  $|b_k|$  are also constructible from  $S$ . It follows (ex. 3, §1) that a segment of length  $|b_i|$ , and therefore also the point  $(b_i, 0)$ , is constructible from  $S$ .

If one of  $b_j$  and  $b_k$  is positive and the other negative, then, if  $|b_j| > |b_k|$ ,  $|b_i| = |b_j| - |b_k|$ . Proceeding as before (using ex. 2(b), §1), we see that  $(b_i, 0)$  is constructible from  $S$ .

(c)  $b_i = b_j - b_k$  or  $b_j b_k$  or  $b_j/b_k$ . The desired result follows as in case (b).

(d)  $b_i = \pm \sqrt{b_j}$  where  $j < i$ . Since  $b_i$  is real,  $b_j > 0$ . As in case (b) (using ex. 2(c), §1), a segment of length  $|b_i| = \sqrt{b_j}$  is constructible from  $S$ . The same, therefore, is true of  $(b_i, 0)$ .

By the principle of mathematical induction, it follows that each of the points  $(b_1, 0), \dots, (b_p, 0)$  is constructible from  $S$ . Since  $r = b_p$ ,  $(r, 0)$  is constructible from  $S$ .

Now consider any figure of  $T$ . Suppose it is the point  $(r_i, r_j)$ . We have seen that  $(r_i, 0)$  and  $(0, r_j)$  are constructible from  $S$ . From  $(r_i, 0)$  we can construct  $(0, r_j)$ , and from  $(r_i, 0)$  and  $(0, r_j)$  we can construct  $(r_i, r_j)$ .

Suppose the figure is a line  $r_i x + r_j y + r_k = 0$ . We can determine two points on the line; for instance, if  $r_i \neq 0$ , the points

$\left(-\frac{r_k}{r_i}, 0\right)$  and  $(-(r_k + r_j)/r_i, 1)$ . The coordinates of these points are rational in  $r_i, r_j, r_k$  and, from what we have already proved, are constructible from the points  $(r_i, 0), (r_j, 0), (r_k, 0)$ . Since  $(r_i, 0), (r_j, 0), (r_k, 0)$  are constructible from  $S$ , it follows (ex. 3, §1) that the two points on the line are constructible from  $S$ . Since the line is constructible from these two points, the line is also constructible from  $S$ .

We leave it to the reader to complete the proof by showing that every ray, segment or circle of  $T$  is constructible from  $S$ .

*Example* Show that it is possible with ruler and compasses to construct a right triangle with area  $A > 0$  having a hypotenuse of length  $a > 0$ , provided  $a \geq 2\sqrt{A}$ .

Let  $x$  and  $y$  be the lengths of the arms. Then  $xy = 2A$  and  $x^2 + y^2 = a^2$ . Solving these equations simultaneously, we obtain as one solution

$$x = \sqrt{a^2 + \frac{\sqrt{a^4 - 16A^2}}{2}}$$

$$y = 2A \sqrt{\frac{2}{a^2 + \sqrt{a^4 - 16A^2}}}$$

Since  $x$  and  $y$  are obtainable from  $a$  and  $A$  by rational operations and extractions of real square roots, the construction is possible.

### Exercises

- \*1 If  $c$  is rational in  $b_1, b_2, \dots$  and each  $b_i$  is rational in  $a_1, a_2, \dots$ , then  $c$  is rational in  $a_1, a_2, \dots$ .
- \*2 If  $c$  is obtainable from  $b_1, b_2, \dots$  by rational operations and extractions of square roots (or real square roots) and each  $b_i$  is obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots (or real square roots), then  $c$  is obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots (or real square roots).
- \*3 If  $a, b, c$  are obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots, and  $a \neq 0$ , then the roots of  $ax^2 + bx + c = 0$  are also so obtainable.
- 4 All the numbers rational in  $a_1, a_2, \dots$  form a field, if not all the  $a$ 's are zero.
- 5 All the numbers obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots form a field, if  $a_i \neq 0$  for some  $i$ .
- 6 If  $a_1, a_2, \dots$  are in field  $\mathfrak{F}$  and  $r$  is rational in the  $a$ 's, then  $r$  is in  $\mathfrak{F}$ .

**3. Problem of trisecting an angle** Suppose angle  $A$  given. With ruler and compasses an angle  $A'$  can be constructed congruent to  $A$  with the positive part of the  $x$  axis as the initial side of  $A'$ . By laying off on the terminal side of  $A'$  a segment of length 1 and drawing a line perpendicular to the  $x$  axis, a segment of length  $|\cos A|$  can be constructed. This is a ruler and compass construction.

Conversely, if  $a$  is a given real number such that  $|a| < 1$ , an angle whose cosine is  $a$  can be constructed with ruler and compasses. We may take the positive part of the  $x$  axis as the initial side and as the terminal side the ray which has the origin as endpoint and which passes through the point  $(a, \sqrt{1-a^2})$ .

Thus, an angle  $A$  is constructible with ruler and compasses from given elements if and only if a segment of length  $|\cos A|$  is so constructible.

The problem of trisecting a given angle  $A$ , therefore, is equivalent to the problem of constructing a segment of length  $|\cos A/3|$  from a segment of length  $|\cos A|$ . Hence, this construction is possible with ruler and compasses if and only if  $\cos A/3$  is obtainable from  $\cos A$  by rational operations and extractions of real square roots.

By the triple angle formula of trigonometry,

$$\cos A = 4 \cos^3 \frac{A}{3} - 3 \cos \frac{A}{3}$$

If  $x = \cos A/3$ , then  $4x^3 - 3x - \cos A = 0$ .

Thus, if  $A$  can be trisected with ruler and compasses, this equation has a root obtainable from  $\cos A$  by rational operations and extractions of real square roots. We shall show, by a criterion developed in §5, that this is not always possible.

**4. Multiple square roots** "Obviously" the "two-storied" square root  $\sqrt{6-4\sqrt{2}}$  is more "complicated" than  $2-\sqrt{2}$  which involves only one square root. But this complication is only an apparent one since, in fact, the two expressions are equal [for  $(2-\sqrt{2})^2 = 6-4\sqrt{2}$ ]. This raises the question of classifying multiple square roots according to their complexity. We shall discuss one way of classifying them that will be useful in subsequent paragraphs.



If  $r$  is obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots, then, by definition, there exists a sequence  $b_1, b_2, \dots, b_p$  such that  $b_p = r$  and each  $b_i$  is rational in the  $a$ 's and preceding  $b$ 's or is a square root of a preceding  $b$ . There may be many such sequences.

In each sequence there is a certain number, say  $q$  (possibly none) of  $b$ 's which are not rational in the  $a$ 's and preceding  $b$ 's. Let  $n \geq 0$  be the smallest value that it is possible for  $q$  to have by using different sequences for obtaining  $r$ . For convenience, we shall say that  $r$  is a square root of order  $n$  in the  $a$ 's. (If  $n = 0$  then  $r$  is rational in the  $a$ 's.)

Suppose  $n > 0$ . Let  $b_1, b_2, \dots, b_p$ , where  $b_p = r$ , be a sequence such as described above with exactly  $n$  of the  $b$ 's not rational in the  $a$ 's and preceding  $b$ 's, and let  $b_k$  be the last such  $b$ . Then  $b_k = \sqrt{b_l}$  (either square root), where  $1 \leq l \leq k-1$ .

For subsequent use, we show that  $b_i = \alpha_i + \beta_i \sqrt{b_l}$  ( $i = 1, 2, \dots, p$ ) where  $\alpha_i$  and  $\beta_i$  are rational in the  $a$ 's and  $b_1, b_2, \dots, b_{k-1}$ .

For  $i = 1$  this is obvious. For  $b_1$  must be one of the  $a$ 's, say  $a_u$ , and we may write  $b_1 = \alpha_1 + (a_u - \alpha_u) \sqrt{b_l}$ .

Proceeding by mathematical induction, suppose it true for  $i = 1, 2, \dots, j-1$ , and let  $i = j$ .

If  $j < k$ , we may write  $b_j = b_l + (b_j - b_l) \sqrt{b_l}$ .

If  $j = k$ , we may write  $b_j = (b_l - b_l) + (b_l/b_l) \sqrt{b_l}$ . (Note that  $b_l \neq 0$ , for if  $b_l = 0$  then  $b_l \div 0 = b_1 - b_1$ , so that  $b_k$  would be rational in the preceding  $b$ 's.)

Suppose  $j > k$ . Since  $b_l$  is the last  $b$  which is not rational in the  $a$ 's and preceding  $b$ 's, therefore  $b_j$  is obtainable from the  $a$ 's and  $b_1, b_2, \dots, b_{j-1}$  by a finite number of additions, multiplications, subtractions and divisions. Each of the numbers  $a_1, a_2, \dots$  and  $b_1, b_2, \dots, b_{j-1}$  has the desired form. Hence it will follow that  $b_j$  has the desired form if we show that whenever we add, multiply, subtract or divide two numbers of this form we obtain a number of the same form.

Consider, for instance, the quotient (the other cases are simpler)

$$x = \frac{\alpha + \beta \sqrt{b_l}}{\gamma + \delta \sqrt{b_l}}$$

where  $\alpha, \beta, \gamma, \delta$  are rational in the  $a$ 's and  $b_1, \dots, b_{k-1}$  and  $\gamma + \delta \sqrt{b_l} \neq 0$ .

$\gamma - \delta \sqrt{b_i} \neq 0$ . For, if  $\gamma - \delta \sqrt{b_i} = 0$  then, by transposing and squaring,  $\gamma^2 = \delta^2 b_i$ . If  $\delta = 0$  then  $\gamma = 0$ , contradicting  $\gamma + \delta \sqrt{b_i} \neq 0$ . If  $\delta \neq 0$  then  $b_i = \gamma^2/\delta^2$ , so that  $b_k = \sqrt{b_i} = \pm \frac{\gamma}{\delta}$ ; hence  $b_k$  is rational in the  $a$ 's and  $b_1, \dots, b_{k-1}$ , which contradicts the definition of  $b_k$ .

Since  $\gamma - \delta \sqrt{b_i} \neq 0$ ,

$$x = \frac{\alpha + \beta \sqrt{b_i}}{\gamma + \delta \sqrt{b_i}} \frac{\gamma - \delta \sqrt{b_i}}{\gamma - \delta \sqrt{b_i}} = \frac{\alpha\gamma - \beta\delta b_i}{\gamma^2 - \delta^2 b_i} + \frac{\beta\gamma - \alpha\delta}{\gamma^2 - \delta^2 b_i} \sqrt{b_i}$$

from which we see that  $x$  has the desired form. Thus, in every case  $b_i$  has the desired form.

By the principle of mathematical induction, our statement is proved.

## 5. Criterion for cubics Let $f(x) \equiv ax^3 + bx^2 + cx + d, a \neq 0$ .

### THEOREM

*If  $a, b, c, d$  are rational in  $a_1, a_2, \dots$  then  $f(x)$  has a root obtainable from the  $a_i$  by rational operations and extractions of square roots if and only if it has a root which is rational in the  $a_i$ .*

(The square roots need not be real.)

*Proof:* If  $f(x)$  has a root which is rational in the  $a_i$ , then this root is also obtainable from the  $a_i$  by rational operations and extractions of square roots (with no square roots actually needed). Hence, one part of the theorem is obviously true and, in fact, trivial.

To establish the converse, suppose  $f(x)$  has a root obtainable from the  $a_i$  by rational operations and extractions of square roots. Of all the roots of  $f(x)$  so obtainable, let  $r$  be one of lowest order, say  $n$ . We show that  $n = 0$ , i.e., that  $r$  is rational in the  $a_i$ .

Suppose  $n > 0$  and that, continuing where we left off in §4,  $r = \alpha + \beta \sqrt{b_i}$  where  $\alpha$  and  $\beta$  are rational in the  $a_i$  and  $b_1, b_2, \dots, b_{k-1}$ . Then

$$\begin{aligned} f(r) &= f(\alpha + \beta \sqrt{b_i}) = a(\alpha + \beta \sqrt{b_i})^3 + b(\alpha + \beta \sqrt{b_i})^2 \\ &\quad + c(\alpha + \beta \sqrt{b_i}) + d \\ &= A + B \sqrt{b_i} \end{aligned}$$

$$\begin{aligned}\text{where } A &= a\alpha^3 + 3a\beta^2\alpha b_1 + b\alpha^2 + b\beta^2b_1 + c\alpha + d \\ B &= 3a\alpha^2\beta + a\beta^2b_1 + 2b\alpha\beta + c\beta\end{aligned}$$

$A$  and  $B$  are obtainable from  $a, b, c, d, \alpha, \beta, b_1$  by rational operations. Also,  $a, b, c, d, \alpha, \beta, b_1$  are rational in the  $a_i$  and  $b_1, b_2, \dots, b_{k-1}$ . Therefore (ex. 1, §2),  $A$  and  $B$  are rational in the  $a_i$  and  $b_1, b_2, \dots, b_{k-1}$ .

Since  $f(r) = 0$ ,  $A + B\sqrt{b_1} = 0$ . If  $B \neq 0$ , then  $b_k = \sqrt{b_1} = -\frac{A}{B}$ , so that  $b_k$  would be rational in the  $a_i$  and  $b_1, b_2, \dots, b_{k-1}$ , which is contrary to the definition of  $b_k$ . Therefore,  $B = 0$  and, consequently,  $A = 0$ . Also

$$\begin{aligned}f(\alpha - \beta\sqrt{b_1}) &= a(\alpha - \beta\sqrt{b_1})^3 + b(\alpha - \beta\sqrt{b_1})^2 \\ &\quad + c(\alpha - \beta\sqrt{b_1}) + d = A - B\sqrt{b_1} = 0\end{aligned}$$

Thus,  $\alpha - \beta\sqrt{b_1}$  is a root of  $f(x)$ .

$\alpha - \beta\sqrt{b_1} \neq \alpha + \beta\sqrt{b_1}$ . For, if they were equal then  $2\beta\sqrt{b_1} = 0$ , so that either  $\beta = 0$  or  $b_1 = 0$ . But  $b_1 = b_1^2 \neq 0$ . Hence,  $\beta = 0$ . Therefore,  $r = \alpha$ . This is impossible since  $\alpha$  is of order  $n - 1$  or less in the  $a_i$  and  $b_1, \dots, b_{k-1}$  and  $r$  is of order  $n$ .

Thus,  $\alpha + \beta\sqrt{b_1}$  and  $\alpha - \beta\sqrt{b_1}$  are distinct roots of  $f(x)$ . If  $s$  is the third root, then  $(\alpha + \beta\sqrt{b_1}) + (\alpha - \beta\sqrt{b_1}) + s = -\frac{b}{a}$  (§4, Ch. 3). Hence  $s = -(b/a) - 2\alpha$ .

Since  $a, b, \alpha$  are rational in the  $a_i$  and  $b_1, \dots, b_{k-1}$ ,  $s$  is also (ex. 1, §2). But in  $b_1, b_2, \dots, b_{k-1}$  there are only  $n - 1$   $b$ 's which are not rational in the  $a_i$  and preceding  $b$ 's. It follows that  $s$  is a square root in the  $a_i$  of order  $n - 1$  or less.

This is impossible since, by supposition,  $f(x)$  has no root of order less than  $n$ .

Since the supposition that  $n > 0$  has led to a contradiction,  $n = 0$ , and the theorem is proved.

*Example* Show that  $8x^3 - 6x - 1 = 0$  has no root obtainable from rational numbers by rational operations and extractions of square roots.

If there is such a root then, by the theorem, since the coefficients are rational numbers, there is a root obtainable from rational numbers by rational operations only. Any such root is necessarily a

rational number. But the only possible rational roots are  $\pm 1$ ,  $\pm \frac{1}{2}$ ,  $\pm \frac{1}{4}$ ,  $\pm \frac{1}{8}$  (§2, Ch. 5), and none of these is a root.

**6. Impossibility of certain constructions** We can now show that certain constructions are impossible with ruler and compasses.

(1) **Trisection of angle** To trisect an angle of  $60^\circ$  it must be possible to obtain a root of  $4x^3 - 3x - \frac{1}{2} = 0$  from  $\cos 60^\circ = \frac{1}{2}$  by rational operations and extractions of real square roots (§3). But this equation has no such root (example, §5).

(2) **Construction of certain regular polygons** (a) Suppose it were possible with ruler and compasses to construct a regular polygon of 18 sides, having been given a unit segment. The center of the circumscribed circle could be obtained as the intersection of the perpendicular bisectors of adjacent sides. By joining adjacent vertices to the center we have an angle of  $20^\circ$  constructed with ruler and compasses. But this, as we saw in (1), is impossible.

(b) Suppose it were possible with ruler and compasses to construct a regular polygon of 7 sides, having been given a unit segment. As in (a), we would have an angle  $A = 360^\circ/7$  constructed at the center of the circumscribed circle by means of ruler and compasses.

If  $x = \cos A$ , then

$$\begin{aligned}\cos 3A &= 4 \cos^3 A - 3 \cos A = 4x^3 - 3x \\ \cos 4A &= 2 \cos^2 2A - 1 = 2(2 \cos^2 A - 1)^2 - 1 \\ &= 2(2x^2 - 1)^2 - 1 = 8x^4 - 8x^2 + 1\end{aligned}$$

Since  $3A + 4A = 360^\circ$ ,  $\cos 4A = \cos 3A$ . Hence

$$\begin{aligned}8x^4 - 8x^2 + 1 &= 4x^3 - 3x \\ 8x^4 - 4x^3 - 8x^2 + 3x + 1 &= 0\end{aligned}$$

One root of this equation is  $x = 1$ . Obviously  $\cos A \neq 1$ . The other roots satisfy

$$8x^3 + 4x^2 - 4x - 1 = 0$$

The only possible rational roots of this equation are  $\pm 1$ ,  $\pm \frac{1}{2}$ ,  $\pm \frac{1}{4}$ ,  $\pm \frac{1}{8}$  (§2, Ch. 5), and none of these is a root. Since it has no rational root, it has no root obtainable from 1 by rational operations and extractions of real square roots.

Therefore,  $x$  cannot be constructed with ruler and compasses.

(3) **Duplication of cube** The problem is to construct with ruler and compasses a cube having twice the volume of a cube with a given edge. Taking an edge of the given cube as a unit segment and  $x$  as an edge of the required cube, we have  $x^3 - 2 = 0$ .

Thus, the problem is to find a positive root of this equation obtainable from 1 by rational operations and extractions of real square roots. But this equation has no such root, since it does not have a rational root.

### Exercises

1 Show that the roots of the following can be obtained from the coefficients by rational operations and extractions of square roots:

- a)  $x^3 - 3x^2 - 3x + 1 = 0$                       d)  $x^2 - x - \sqrt{2} = 0$   
 b)  $2x^3 - x^2 + 2x - 1 = 0$                       e)  $x^3 - x - 4 + \sqrt[3]{4} = 0$   
 c)  $x^3 - ax^2 + (1 - 2a^2)x - 2a = 0$         f)  $x^3 - ix^2 + 2x - 2i = 0$

2 Show that the following have no roots obtainable from the coefficients by rational operations and extractions of square roots:

- a)  $x^3 - 7x^2 + x - 1 = 0$   
 b)  $2x^3 - 3x + 2 = 0$   
 c)  $x^3 + ax^2 + ax + 2 = 0$ ,  $a$  an integer different from 3  
 d)  $x^3 + ax + a = 0$ ,  $a$  an integer different from 0 and  $-8$   
 e)  $x^3 + 2i = 0$  (Hint: There is no root  $a + bi$  where  $a$  and  $b$  are rational.)  
 f)  $x^3 - 3x + \sqrt{3} = 0$  (Hint: There is no root  $a + b\sqrt{3}$  where  $a$  and  $b$  are rational)

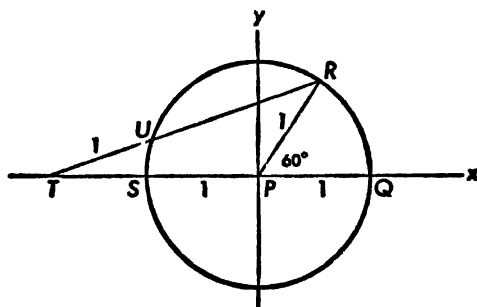
3 Show that it is impossible by rational operations and extractions of square roots to obtain:

- a)  $\sqrt[3]{7}$  from 1  
 b)  $3 + \sqrt[3]{5}$  from 1  
 c)  $\frac{1}{1 + \sqrt[3]{3}}$  from 1  
 d) A cube root of  $5i$  from  $i$   
 e)  $\sqrt[3]{2}$  from  $\sqrt{2}$   
 f)  $A + B$ , where  $A$  and  $B$  are the real cube roots of  $\frac{1}{2} + \frac{1}{2}\sqrt{5\frac{2}{27}}$  and  $\frac{1}{2} - \frac{1}{2}\sqrt{5\frac{2}{27}}$ , from 1 (Use ex. 2, §4, Ch. 8.)
- 4 If  $r_1, r_2, r_3$  are the roots of  $x^3 + bx^2 + cx + d = 0$ , then
- $r_3$  is rational in  $r_1, r_2, b, c, d$
  - $r_2$  and  $r_3$  are obtainable from  $r_1, b, c, d$  by rational operations and extractions of square roots.

- 5 Suppose  $b, c, d$  are rational in  $a_1, a_2, \dots$ . Prove: If one root of  $x^3 + bx^2 + cx + d = 0$  is obtainable from the  $a$ 's by rational operations and extractions of square roots, then all the roots are so obtainable.
- 6 Prove: If a cubic has a multiple root, then all its roots are obtainable from its coefficients by rational operations.
- 7 Prove: If a cubic has a root whose reciprocal is a root, then the roots of the cubic are obtainable from the coefficients by rational operations and extractions of square roots.
- 8 Show that it is possible with ruler and compasses to:
- Trisect an angle whose cosine is  $11/16, 143/343, -9/16, -47/128, 23/27$ .
  - Find the foci of an ellipse when its center and major and minor axes are given.
  - Find the points of intersection of an ellipse, given its center and major and minor axes, with a line through its center making a  $45^\circ$  angle with the major axis.
  - Construct a regular pentagon.
  - Construct a regular polygon of  $2^k n$  sides if a regular polygon of  $n$  sides can be constructed and  $k$  is a positive integer.
  - Construct a regular polygon of  $ab$  sides if  $a$  and  $b$  are relatively prime and regular polygons of  $a$  and  $b$  sides are constructible [Hint: Let  $am + bn = 1$  (§13, Ch. 2).]
  - Construct a regular polygon of  $a$  sides if a regular polygon of  $n$  sides can be constructed and  $a$  is a factor of  $n$ .
- 9 Show that it is impossible with ruler and compasses to:
- Trisect an angle of  $120^\circ$ .
  - Construct a regular polygon of 9 sides.
  - Construct an angle of  $10^\circ$ .
  - Construct an angle of  $1^\circ$ .
  - Construct a regular polygon of 21 sides.
  - Trisect an angle whose cosine is  $2/3, 5/24, 1/34, p/3$  where  $p$  is an odd integer.
  - Trisect an angle whose cosine is  $p/q$  where  $p$  and  $q$  are relatively prime integers greater than 1 and  $q$  is not divisible by the cube of an integer greater than 1.
  - Construct a line segment of length  $\sqrt[3]{a/b}$  where  $a$  and  $b$  are relatively prime integers and  $\sqrt[3]{a/b}$  is irrational.
  - Find the points of intersection of the semicubical parabola  $y^2 = x^3$  and the circle  $x^2 + y^2 = 1$ .
  - Construct the edges of a closed rectangular box with a square base, a volume of 10 cubic units and a total surface area of 40 square units.
- 10 From each of the four corners of a rectangular piece of cardboard 4 inches wide and 5 inches long a square is to be cut. The edges of the

piece remaining are to be folded up so that a box is formed with an open top. Prove: (a) If the box is to have a volume of 6 cubic inches, then an edge of the square can be constructed with ruler and compasses, but (b) if the volume is to be 4 cubic inches, then the edge cannot be so constructed.

- 11 Show that (a) it is impossible with ruler and compasses to construct the edges of a completely enclosed rectangular box with a volume of 5 cubic units, a total surface area of 24 square units, and the sum of the lengths of the edges 28 units, but (b) it is possible if the volume is 5 cubic units, the total surface area 24 square units and the sum of the lengths of the edges 32 units.
- 12 Show that (a) it is impossible with ruler and compasses to construct the radius and altitude of a right circular cylinder whose total surface area is  $10\pi$  square units and whose volume is  $3\pi$  cubic units, but (b) it is possible if the total surface area is  $20\pi$  square units and the volume  $3\pi$  cubic units. (The volume is  $\pi r^2 h$  and the lateral area  $2\pi r h$ , where  $r$  and  $h$  are the radius and altitude.)
- 13 Show that (a) it is impossible with ruler and compasses to construct the radius and altitude of a right circular cone whose lateral area is  $12\pi$  square units and whose volume is  $2\pi$  cubic units, but (b) it is possible if the lateral area is  $6\pi$  square units and the volume  $3\pi$  cubic units. (The volume is  $\frac{1}{3}\pi r^2 h$  and the lateral area  $\pi r s$ , where  $r$  is the radius,  $h$  the altitude,  $s$  the slant height.)
- 14 Given a circle of radius 1, center at  $P$ , with angle  $QPR = 60^\circ$  at the center (see diagram). Show that it is not possible with ruler and compasses to find points  $T'$  and  $U$  such that:



- a)  $U$  is on the circle.
- b)  $T$  is outside the circle and on the ray  $PS$  with endpoint at  $P$ .
- c) Segment  $TU$  has length 1.
- d)  $T, U, R$  are collinear.

[Hint: Let  $T$  be  $(x, 0)$  and  $U$  be  $(y, z)$ . Write out conditions (a), (c), (d). Eliminate  $y$  and  $z$  and obtain an equation in  $x$ .]

**7. Criterion for quartics** Let  $f(x) \equiv x^4 + ax^3 + bx^2 + cx + d$  where  $a, b, c, d$  are rational in  $a_1, a_2, \dots$ .

### THEOREM

*If  $f(x)$  has a root obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots, and this root is not rational in the  $a_i$ , then all the roots of  $f(x)$  are obtainable from the  $a_i$  by rational operations and extractions of square roots.*

*Proof:* Let  $r$  be a root of  $f(x)$  which is a square root of order  $n > 0$  in the  $a_i$ .

Exactly as in §5, if  $r = \alpha + \beta \sqrt{b_1}$  then  $s = \alpha - \beta \sqrt{b_1}$  is another root of  $f(x)$  distinct from  $r$ . Let  $x_1$  and  $x_2$  be the remaining two roots of  $f(x)$ .

From the relations between the roots and the coefficients (§4, Ch. 3),

$$\begin{aligned}x_1 + x_2 + r + s &= -a \\x_1x_2 + (r+s)(x_1+x_2) + rs &= b\end{aligned}$$

Eliminating  $x_2$  we obtain

$$x_1^2 + (a + r + s)x_1 + b + (r + s)^2 + a(r + s) - rs = 0$$

This is a quadratic equation in  $x_1$  with coefficients which are rational in  $a, b, c, d, r, s$ . Since  $a, b, c, d, r, s$  are obtainable from the  $a_i$  by rational operations and extractions of square roots, the coefficients of the quadratic equation are also so obtainable (ex. 2, §2).

Thus (ex. 3, §2),  $x_1$  is obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots.

Since  $x_2 = -a - r - s - x_1$ ,  $x_2$  is also so obtainable, and the theorem is proved.

*Remark* If  $n = 0$  the conclusion of the theorem does not follow. For example (§6, (2), (b))  $x^4 - \frac{1}{2}x^3 - x^2 + \frac{3}{2}x + \frac{1}{2} = 0$  has the root  $x = 1$  and no other root obtainable from rational numbers by rational operations and extractions of square roots.

### THEOREM

*All the roots of  $f(x)$  are obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots if and only if the resolvent cubic has a root which is rational in the  $a_i$ .*



We recall (§7 and 8, Ch. 8)

(a) the resolvent cubic is  $g(y) \equiv y^3 - by^2 + (ac - 4d)y + 4bd - a^2d - c^2$

(b) if  $y_i$  is a root of  $g(y)$ , then

$$f(x) \equiv (x^2 + \frac{1}{2}ax + \frac{1}{2}y_i + \lambda_i x + \mu_i) (x^2 + \frac{1}{2}ax + \frac{1}{2}y_i - \lambda_i x - \mu_i)$$

$$\text{where } \lambda_i^2 = y_i + \frac{1}{4}a^2 - b, 2\lambda_i\mu_i = \frac{1}{2}ay_i - c, \mu_i^2 = \frac{1}{4}y_i^2 - d$$

(c) if  $x_1, x_2, x_3, x_4$  are the roots of  $f(x)$ , then

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_2x_4, \quad y_3 = x_1x_4 + x_2x_3$$

are the roots of  $g(y)$ .

We remark that, since  $a, b, c, d$  are rational in the  $a$ , the coefficients of  $g(y)$  are also.

We now prove the theorem.

*Part 1* Suppose  $x_1, x_2, x_3, x_4$  are obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots. From the expressions for  $y_1, y_2, y_3$  in (c) above (and ex. 2, §2) it follows that all the roots of  $g(y)$  are also so obtainable. From the criterion for cubics (§5) it follows that  $g(y)$  has a root which is rational in the  $a$ .

*Part 2* Suppose  $g(y)$  has a root  $y_i$  which is rational in  $a_1, a_2, \dots$ . Then, from (b) above,  $\lambda_i$  and  $\mu_i$  are obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots. Thus, the coefficients in the quadratic factors of  $f(x)$  are also so obtainable. It follows (ex. 3, §2) that  $x_1, x_2, x_3, x_4$ , which are the roots of the quadratic factors, are also obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots.

### THEOREM

*$f(x)$  has a root obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots if and only if  $f(x)$  or  $g(y)$  has a root which is rational in the  $a$ .*

*Part 1* Suppose  $f(x)$  has a root obtainable from the  $a$  by rational operations and extractions of square roots. If this root is rational in the  $a$ , there is nothing more to be proved. If not, then, by the first theorem of this paragraph, all the roots of  $f(x)$  are obtainable from the  $a$ , by rational operations and extractions of

square roots. Therefore, by the second theorem,  $g(y)$  has a root which is rational in the  $a_i$ .

**Part 2** Suppose one (or both) of  $f(x)$  and  $g(y)$  has a root which is rational in the  $a_i$ . If  $f(x)$  has such a root, there is nothing more to be proved. If  $g(y)$  has such a root, then, by the preceding theorem, all the roots of  $f(x)$  are obtainable from  $a_1, a_2, \dots$  by rational operations and extractions of square roots.

**Example 1** Show that  $f(x) \equiv x^4 + x + 1$  has no root obtainable from rational numbers by rational operations and extractions of square roots.

Neither  $f(x)$  nor the resolvent cubic  $g(y) \equiv y^3 - 4y - 1$  has a rational root. Therefore, the preceding theorem applies.

**Example 2** Show that  $\sqrt[3]{5\sqrt{2}-7}$  is obtainable from rational numbers by rational operations and extractions of square roots.

Let  $x = \sqrt[3]{5\sqrt{2}-7}$ . Then

$$\begin{aligned}x^3 &= 5\sqrt{2} - 7 \\x^3 + 7 &= 5\sqrt{2}\end{aligned}$$

Squaring both sides and transposing all terms to the left,

$$x^6 + 14x^3 - 1 = 0$$

But  $x^6 + 14x^3 - 1 \equiv (x^2 + 2x - 1)(x^4 - 2x^3 + 5x^2 + 2x + 1)$

The roots of the quadratic factor are obtainable from rational numbers by rational operations and extractions of square roots.

For the quartic factor, the resolvent cubic is  $y^3 - 5y^2 - 8y + 12$ , which has  $y = 1$  as a root. By the second theorem above, all the roots of the quartic are obtainable from rational numbers by rational operations and extractions of square roots.

Since  $x$  is a root of one of the factors, the desired result is established. (Actually,  $x = \sqrt{2} - 1$ .)

### Exercises

1 Show that the roots of the following can be obtained from the coefficients by rational operations and extractions of square roots:

a)  $x^4 - x^3 - 3x^2 + x + 2 = 0$

b)  $x^4 + 3x^3 + 4x^2 + 3x + 3 = 0$

- c)  $x^4 - (1+i)x^3 + 2ix^2 + (1-i)x - 1 = 0$   
 d)  $x^4 - \sqrt{2}x^3 + (1 + \sqrt{2})x^2 - 2x + \sqrt{2} = 0$  ,  
 e)  $x^4 - 2x^3 - 7x^2 + 2x + 1 = 0$
- 2 Show that no root is obtainable from the coefficients by rational operations and extractions of square roots:
- a)  $x^4 + 3x^3 - 2 = 0$   
 b)  $x^4 + 2x^2 + x + 1 = 0$   
 c)  $x^4 + x^3 + x^2 + x - 1 = 0$   
 d)  $x^4 + x^3 + 2^n = 0$ ,  $n$  a positive integer  
 e)  $x^4 + px + p = 0$ ,  $p$  a prime integer other than 3 or 5
- 3 If a quartic has a multiple root, then all its roots are obtainable from the coefficients by rational operations and extractions of square roots.
- 4 Prove: The points of intersection of the parabolas  $y = x^2$  and  $y^2 = x - 2$  cannot be constructed with ruler and compasses.
- 5 Show that it is impossible with ruler and compasses to inscribe in a circle of radius 1 an isosceles triangle with area  $\frac{1}{4}$ .
- 6 Prove: It is impossible with ruler and compasses to construct one fifth of an acute angle whose cosine is  $\frac{1}{64}$ . (Hint: Let  $x = \cos A$ . Then  $16x^5 - 20x^3 + 5x = \cos 5A = \frac{1}{64}$ . Find a rational root and reduce the degree.)
- 7 Show that  $\sqrt[4]{6\sqrt{3} - 10}$  and  $\sqrt[3]{20 - 14\sqrt{2}}$  are obtainable from rational numbers by rational operations and extractions of square roots.
- 8 Prove: If the resolvent cubic of a quartic has a root obtainable from the coefficients of the cubic by rational operations and extractions of square roots, then all the roots of the quartic are obtainable from the coefficients of the quartic by rational operations and extractions of square roots. Show, using  $x^4 + \sqrt[3]{2}x^3 + \frac{1}{4}(-1 + \sqrt{33})x + \frac{1}{16}\sqrt[3]{2}(-1 + \sqrt{33})$  as an example, that the converse is not true.

**8. Remarks on angle trisection** We have seen that certain angles cannot be trisected with ruler and compasses. (Some angles, however, can; for instance,  $90^\circ$ .) But every once in a while someone claims to have a method for trisecting every angle. The fallacy usually lies in one of the following remarks:

(1) The method is not one for trisecting every angle theoretically exactly but one which permits approximate trisection. It may even be that by the method we can, with ruler and compasses only, approximate to one-third of a given angle as closely as we wish. Nevertheless, it is not angle trisection.

As an example of such a method, consider the following: Let  $n$  be a positive integer and  $A$  a given angle. Divide  $A$  into  $2^n$  equal parts. This can be done with ruler and compasses, since it can be accomplished by  $n$  bisections.

By the binomial theorem,

$$\begin{aligned} 2^n &= (3 - 1)^n = 3^n + n3^{n-1}(-1) + \frac{n(n-1)}{2!} 3^{n-2}(-1)^2 + \\ &\quad \cdot \cdot \cdot + n3(-1)^{n-1} + (-1)^n \\ &= 3m + (-1)^n \end{aligned}$$

where  $m$  is a positive integer. Hence,

$$\frac{2^n}{3} = m + \frac{(-1)^n}{3}$$

If we take  $m$  of the  $2^n$  equal parts into which  $A$  has been divided, we have

$$\begin{aligned} B &= m \frac{A}{2^n} = \left[ \frac{2^n}{3} - \frac{(-1)^n}{3} \right] \frac{A}{2^n} = \frac{A}{3} - \frac{(-1)^n A}{3 \cdot 2^n} \\ B - \frac{A}{3} &= \frac{(-1)^{n+1} A}{3 \cdot 2^n} \end{aligned}$$

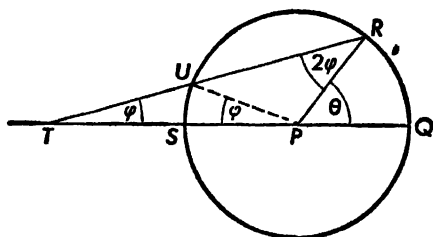
Thus,  $B$  is less than  $A/3$  or exceeds it, depending upon whether  $n$  is even or odd, by the amount  $\frac{A}{3 \cdot 2^n}$ . By taking  $n$  large enough we can make this difference as small as we please.

(2) The method requires the use of instruments or devices other than ruler and compasses. Such methods have been known for a long time. The following is due to Archimedes.

Let  $\theta$  be a given angle. Bisecting  $\theta$  a sufficient number of times, if necessary, we may and do suppose that  $\theta$  is an acute angle.

Draw a circle with center at the vertex  $P$  of  $\theta$ , intersecting the sides of the angle at points  $Q$  and  $R$ . Extend  $QP$  through  $P$  to meet the circle again at point  $S$ .

On a straightedge lay off a distance  $TU$  equal to the radius  $PQ$ . Keeping the point  $T$  outside the circle and always on the ray  $PS$  with endpoint at  $P$ , and keeping point  $U$  on the semicircle on which  $R$  lies, maneuver the straightedge, by sliding  $T$  along the ray  $PS$  and sliding  $U$  along the semicircle, until  $T$ ,  $U$ , and  $R$  are collinear.



If  $\angle PTR = \varphi$ , then, we say,  $\varphi = \frac{1}{3}\theta$ . For,

$\angle SPU = \varphi$  (since triangle  $TUP$  is isosceles, by construction)

$\angle PUR = \angle PQR$  (since triangle  $PUQ$  is isosceles)

$\angle PUR = \angle PTR + \angle SPU$  (since  $\angle PUR$  is an exterior angle of triangle  $PUR$ )

$\angle PUR = 2\varphi$

$\theta = \varphi + 2\varphi$  (since  $\theta$  is an exterior angle of triangle  $PQR$ )

$= 3\varphi$

This method of angle trisection is theoretically exact but it is not a ruler and compass construction. For certain angles the positions of  $T$  and  $U$  could not possibly be obtained with ruler and compasses only (ex. 14, §6).

**9. Remarks on regular polygons** In any text on elementary plane geometry there are constructions with ruler and compasses for regular polygons of 3, 4, 5, 6, and 8 sides. We know now why none is given for one of 7 sides (§6) or 9 sides (ex. 9(b), §6). We naturally inquire: for what values of  $n$  is it possible to construct an  $n$ -sided regular polygon with ruler and compasses?

From ex. 8, (e) and (f), §6, we see that a regular polygon of  $n$  sides is constructible with ruler and compasses when  $n$  is  $10 = 2 \cdot 5$ ,  $12 = 2^2 \cdot 3$ ,  $15 = 3 \cdot 5$ ,  $16 = 2^4$ .

From ex. 8 (g), §6, we see that a 11-sided regular polygon cannot be constructed with ruler and compasses, since one of 7 sides cannot be. Similarly, an 18-sided regular polygon cannot be constructed, since a 9-sided cannot be.

The complete answer to the question is contained in the following theorem, whose proof we cannot go into: A regular polygon of  $n \geq 3$  sides is constructible with ruler and compasses if and only if  $n = 2^k$

or  $n = 2^k p_1 p_2 \cdots p_l$ , where  $k$  is a non-negative integer and the  $p$ 's are distinct primes each of the form  $2^m + 1$ .

Thus, for  $n = 17 = 2^4 + 1$  the construction is possible, but for  $n = 11$  and  $n = 13$  it is not.

**10. Circle squaring** The three so-called famous problems of antiquity are trisecting an angle, duplicating a cube and squaring a circle. To square a circle is to construct one with the same area as a given square.

If we take a side of the square as a unit segment, the problem is to find a number  $r$  such that  $\pi r^2 = 1$ , i.e., to construct a segment of length  $r = 1/\sqrt{\pi}$ .

If a segment of length  $1/\sqrt{\pi}$  could be constructed with ruler and compasses, then segments of length  $1/\pi$  and  $\pi$  could also be so constructed. Thus, the question is: can  $\pi$  be obtained from 1 by rational operations and extractions of real square roots?

It happens that any number obtainable from 1 by rational operations and extractions of square roots is a root of a non-constant polynomial with rational coefficients (§7, Ch. 10). Any number, real or imaginary, which is a root of such a polynomial is said to be algebraic. All other complex numbers are called transcendental.

It has been proved (first by Lindemann in 1882), although we cannot go into the proof, that  $\pi$  is transcendental. Therefore,  $\pi$  cannot be obtained from 1 by rational operations and extractions of square roots. Hence, squaring the circle cannot be accomplished with ruler and compasses.

## ALGEBRAIC NUMBER FIELDS

**1. Numbers algebraic over a field** A set  $\mathfrak{F}$  of complex numbers (not necessarily including all the complex numbers) is called a field if it contains at least two numbers and whenever  $a$  and  $b$  are in  $\mathfrak{F}$  then  $a + b$ ,  $a - b$ ,  $ab$  and  $a/b$  (if  $b \neq 0$ ) are also in  $\mathfrak{F}$  (§5, Ch. 2).

If  $\mathfrak{F}$  is a field, some complex numbers are roots of non-zero polynomials over  $\mathfrak{F}$  while others may not be. The former play an important role in the theory of polynomials over  $\mathfrak{F}$  since among them will be found the roots of all such polynomials. Such numbers are said to be algebraic over  $\mathfrak{F}$ . That is, a number is algebraic over  $\mathfrak{F}$  if it is a root of a non-zero polynomial with coefficients in  $\mathfrak{F}$ . A number not algebraic over  $\mathfrak{F}$  is said to be transcendental over  $\mathfrak{F}$ .

For example, if  $\mathfrak{F}$  is the field of rational numbers,  $\sqrt{2}$  is algebraic over  $\mathfrak{F}$  since it is a root of  $x^2 - 2$ . On the other hand, it can be shown that  $\pi$  is not a root of any non-zero polynomial with rational coefficients and, therefore, is transcendental over the rational field.

If  $\xi$  is algebraic over  $\mathfrak{F}$  there are many polynomials over  $\mathfrak{F}$  with  $\xi$  as a root. Let  $f(x)$  be one of these of lowest degree, say  $n$ . By dividing  $f(x)$  by its leading coefficient, we obtain a polynomial  $F(x)$  over  $\mathfrak{F}$  of degree  $n$  with leading coefficient 1 which has  $\xi$  as a root. Furthermore, we say,  $F(x)$  is the only such polynomial. For if  $G(x)$  were another, then  $F(x) - G(x)$  would be a polynomial over  $\mathfrak{F}$  with  $\xi$  as a root and of degree less than  $n$ , which is impossible.

The unique polynomial  $F(x)$  is called the minimum polynomial of  $\xi$  over  $\mathfrak{F}$ ;  $\xi$  is said to be of degree  $n$  over  $\mathfrak{F}$ .

$F(x)$  is obviously irreducible over  $\mathfrak{F}$ . For if it were factorable into polynomials with coefficients in  $\mathfrak{F}$  each of lower degree than  $n$ ,  $\xi$  would be a root of one of the factors, which is impossible.

If  $G(x)$  is any polynomial irreducible over  $\mathfrak{F}$  with  $\xi$  as a root, then each of  $F(x)$  and  $G(x)$  divides the other (first theorem of §1, Ch. 5). Hence they differ only by a constant factor. If  $G(x)$  has

leading coefficient 1, the factor is 1. Thus,  $F(x)$  is the only polynomial irreducible over  $\mathfrak{F}$  with leading coefficient 1 which has  $\xi$  as a root.

*Example* Show that  $\xi = \frac{1}{2}(1 - \sqrt[3]{5})$  is of degree 3 over the field  $\mathfrak{F}$  of rational numbers and determine its minimum polynomial over  $\mathfrak{F}$ .

We have

$$\begin{aligned} 2\xi - 1 &= -\sqrt[3]{5} \\ (2\xi - 1)^3 + 5 &= 0 \\ 8\xi^3 - 12\xi^2 + 6\xi + 4 &= 0 \end{aligned}$$

Thus,  $\xi$  is a root of  $f(x) = 4x^3 - 6x^2 + 3x + 2$ .

If  $f(x)$  were reducible over  $\mathfrak{F}$  it would have a linear factor with rational coefficients and, therefore, a rational root. But (§2, Ch. 5) its only possible rational roots are  $\pm 1$ ,  $\pm 2$ ,  $\pm \frac{1}{2}$ ,  $\pm \frac{1}{4}$ , and none of these is a root. Hence,  $f(x)$  is irreducible over  $\mathfrak{F}$ . Therefore,  $F(x) = \frac{1}{4}f(x)$  is the minimum polynomial of  $\xi$  over  $\mathfrak{F}$ .

### Exercises

1 Show that the following are algebraic over the field of rational numbers:

- |                             |                              |
|-----------------------------|------------------------------|
| a) $\sqrt{2} + \sqrt{3}$    | d) $\sqrt[3]{1 - 2\sqrt{5}}$ |
| b) $\sqrt[3]{1 + \sqrt{2}}$ | e) $\sqrt[3]{2} + \sqrt{2}$  |
| c) $\sqrt[3]{3}(1 + i)$     |                              |

2 Show that the following are algebraic and of the stated degrees over the field of rational numbers.

- $a + b\sqrt{2}$ ,  $a$  and  $b$  rational and  $b \neq 0$ , of degree 2 (Hint: See §3, Ch. 5.)
- $1 - \sqrt[4]{3}$ , of degree 3
- $\sqrt{13 + 4\sqrt{3}}$ , of degree 2
- An imaginary cube root of 1, of degree 2
- $a + b\sqrt[3]{4}$ ,  $a$  and  $b$  rational and  $b \neq 0$ , of degree 3

3 Prove: Every imaginary number is of degree 2 over the field of real numbers.

4 Prove: If  $a$  and  $b$  denote any rational numbers, then:

- $1 + \sqrt{3}$  is of degree 2 over the field of numbers of the form  $a + b\sqrt{2}$ .
- $\sqrt{5}$  is of degree 2 over the field of numbers of the form  $a + b\sqrt{3}$ .
- $\sqrt[3]{2}$  is of degree 3 over the field of numbers of the form  $a + b\sqrt{2}$ .

5 Prove: If  $\alpha$  and  $\beta$  are in  $\mathfrak{F}$ , then  $\sqrt{\alpha} - 2\sqrt[4]{\beta}$  is algebraic over  $\mathfrak{F}$  and of degree 8 or less.



- 6 Prove: If  $\xi$  is transcendental over  $\mathfrak{F}$ , then every non-zero integral power of  $\xi$  is transcendental over  $\mathfrak{F}$ .
- \*7 Prove:  $\xi$  is of degree 1 over  $\mathfrak{F}$  if and only if  $\xi$  is in  $\mathfrak{F}$ .
- 8 Prove: If  $\xi$  is of degree  $n$  over  $\mathfrak{F}$  and  $a$  and  $b$  are in  $\mathfrak{F}$ , then each of the following is of degree  $n$  over  $\mathfrak{F}$ :
- |                            |   |
|----------------------------|---|
| a) $a\xi$ if $a \neq 0$    | d) $a\xi + b$ if $a \neq 0$                           |
| b) $\xi + b$               | e) $1/(a\xi + b)$ if $a \neq 0$ and $a\xi + b \neq 0$ |
| c) $1/\xi$ if $\xi \neq 0$ |   |
- 9 Prove: If  $\xi$  is transcendental over  $\mathfrak{F}$  and  $a$  and  $b$  are in  $\mathfrak{F}$ , then each of the following is transcendental over  $\mathfrak{F}$ :
- |                         |                                 |
|-------------------------|---------------------------------|
| a) $a\xi$ if $a \neq 0$ | d) $a\xi + b$ if $a \neq 0$     |
| b) $\xi + b$            | e) $1/(a\xi + b)$ if $a \neq 0$ |
| c) $1/\xi$              |                                 |
- 10 Prove. If  $\xi$  is algebraic over  $\mathfrak{F}$  and  $n$  is a positive integer, then every  $n$ th root of  $\xi$  is algebraic over  $\mathfrak{F}$ .
- 11 Prove: The minimum polynomial of  $\xi$  over  $\mathfrak{F}$  has no multiple root.

**2. Extension of a field** If a field  $\mathfrak{K}$  contains a field  $\mathfrak{F}$ ,  $\mathfrak{K}$  is said to be an extension of  $\mathfrak{F}$ , and we write  $\mathfrak{K} \supset \mathfrak{F}$  or  $\mathfrak{F} \subset \mathfrak{K}$ . For example, the field of complex numbers is an extension of the field of real numbers.

The fact that  $\mathfrak{K}$  is an extension of  $\mathfrak{F}$  does not tell much about  $\mathfrak{K}$  unless something is known about how the numbers in  $\mathfrak{K}$  are related to those in  $\mathfrak{F}$ . For the complex field, for instance, we know that every complex number is uniquely expressible in the form  $a + bi$  where  $a$  and  $b$  are real. It is this fact that enables us to apply our knowledge of real numbers to the study of complex numbers.

If  $\mathfrak{K}$  is an extension of  $\mathfrak{F}$  and if there are  $n$  numbers  $u_1, u_2, \dots, u_n$  in  $\mathfrak{K}$  such that every number in  $\mathfrak{K}$  is uniquely expressible in the form  $c_1u_1 + c_2u_2 + \dots + c_nu_n$  where the  $c$ 's belong to  $\mathfrak{F}$ , then  $\mathfrak{K}$  is said to be of finite degree over  $\mathfrak{F}$ . Specifically,  $\mathfrak{K}$  is said to be of degree  $n$  over  $\mathfrak{F}$  and  $u_1, u_2, \dots, u_n$  is called a basis for  $\mathfrak{K}$  over  $\mathfrak{F}$ . Thus, the complex field is of degree 2 over the real field with  $1, i$  as a basis.

An extension of  $\mathfrak{F}$  may not be of finite degree over  $\mathfrak{F}$  (see ex. 9, §3 or ex. 12, §5). But:

## THEOREM

If  $\mathcal{K}$  is of finite degree over  $\mathcal{F}$ , its degree over  $\mathcal{F}$  is unique.

To prove this, and for other uses, we introduce some terminology and a lemma.

Numbers  $v_1, v_2, \dots, v_m$ ,  $m \geq 1$ , whether in  $\mathcal{F}$  or not, are said to be linearly dependent over  $\mathcal{F}$  if there exist numbers  $a_1, a_2, \dots, a_m$  in  $\mathcal{F}$  and not all zero such that  $a_1 v_1 + a_2 v_2 + \dots + a_m v_m = 0$ . Otherwise they are said to be linearly independent over  $\mathcal{F}$ .

For example, 3 and  $\sqrt{2}$  are linearly dependent over the field of real numbers, since  $(-\sqrt{2})3 + 3\sqrt{2} = 0$ . But they are linearly independent over the field of rational numbers, since  $a_1 3 + a_2 \sqrt{2} = 0$  implies  $a_1 = a_2 = 0$  if  $a_1$  and  $a_2$  are rational.

*Lemma* If  $v_1, \dots, v_m$  are complex numbers and  $w_i = c_{i1}v_1 + c_{i2}v_2 + \dots + c_{im}v_m$  ( $i = 1, 2, \dots, m+1$ ), where the  $c$ 's are in  $\mathcal{F}$ , then  $w_1, w_2, \dots, w_{m+1}$  are linearly dependent over  $\mathcal{F}$ .

*Proof:* If  $m = 1$  then  $w_1 = c_{11}v_1$ ,  $w_2 = c_{21}v_1$ . If  $c_{11} = 0$ , then  $1w_1 + 0w_2 = 0$ . If  $c_{11} \neq 0$ , then  $c_{21}w_1 - c_{11}w_2 = 0$ . In either case,  $w_1$  and  $w_2$  are linearly dependent over  $\mathcal{F}$ .

Proceeding by mathematical induction, suppose the desired result established for  $m = k$ . Then for  $m = k+1$ ,

$$w_i = c_{i1}v_1 + c_{i2}v_2 + \dots + c_{i,k+1}v_{k+1} \quad (i = 1, 2, \dots, k+2)$$

$$w_i - c_{i,k+1}v_{k+1} = c_{i1}v_1 + \dots + c_{ik}v_k$$

The hypothesis of the induction applies to  $w_i - c_{i,k+1}v_{k+1}$  ( $i = 1, 2, \dots, k+1$ ). Hence

$$a_1(w_1 - c_{1,k+1}v_{k+1}) + a_2(w_2 - c_{2,k+1}v_{k+1}) + \dots + a_{k+1}(w_{k+1} - c_{k+1,k+1}v_{k+1}) = 0$$

where  $a_1, \dots, a_{k+1}$  are in  $\mathcal{F}$  and are not all zero. From this,

$$a_1 w_1 + a_2 w_2 + \dots + a_{k+1} w_{k+1} = \lambda v_{k+1}$$

where  $\lambda = a_1 c_{1,k+1} + a_2 c_{2,k+1} + \dots + a_{k+1} c_{k+1,k+1}$ .

If  $\lambda = 0$  there is nothing more to be proved. If  $\lambda \neq 0$  then, by dividing by  $\lambda$ ,

$$\alpha_1 w_1 + \alpha_2 w_2 + \dots + \alpha_{k+1} w_{k+1} = v_{k+1}$$

Since  $a_1, \dots, a_{k+1}, \lambda$  are in  $\mathcal{F}$ , and  $\mathcal{F}$  is a field,  $\alpha_1, \alpha_2, \dots, \alpha_{k+1}$  are in  $\mathcal{F}$ .

Not all the  $\alpha$ 's are zero. To be specific, suppose  $\alpha_1 \neq 0$ .

Proceeding with  $w_2, \dots, w_{k+2}$  as we did with  $w_1, \dots, w_{k+1}$ , we obtain in the same way

$$\beta_2 w_2 + \dots + \beta_{k+2} w_{k+2} = v_{k+1}$$

Subtracting the two expressions obtained for  $v_{k+1}$ , we have

$$\alpha_1 w_1 + (\alpha_2 - \beta_2) w_2 + \dots + (\alpha_{k+1} - \beta_{k+1}) w_{k+1} - \beta_{k+2} w_{k+2} = 0$$

Since  $\alpha_1 \neq 0$ , the desired result is established for  $m = k + 1$ .

By the principle of mathematical induction, the lemma is proved.

Now, to prove the theorem, suppose  $\mathcal{K}$  of degree  $n$  over  $\mathcal{F}$  and also of degree  $m < n$  over  $\mathcal{F}$ . If  $v_1, \dots, v_m$  and  $v_1, \dots, v_m$  are bases for  $\mathcal{K}$  over  $\mathcal{F}$ , then

$$u_i = c_{i1} v_1 + c_{i2} v_2 + \dots + c_{im} v_m \quad (i = 1, 2, \dots, n)$$

where the  $c$ 's are in  $\mathcal{F}$ .

By the lemma, since  $n \geq m + 1$ ,

$$a_1 u_1 + a_2 u_2 + \dots + a_{m+1} u_{m+1} = 0$$

where the  $a$ 's are in  $\mathcal{F}$  and are not all zero.

Thus,

$$0 = 0u_1 + \dots + 0u_n = a_1 u_1 + \dots + a_{m+1} u_{m+1} + 0u_{m+2} + \dots + 0u_n$$

so that 0 is expressed in terms of  $u_1, \dots, u_n$  in two different ways, which contradicts the definition of a basis.

This contradiction proves the theorem.

**3. Algebraic extensions** If  $\mathcal{K}$  is an extension of  $\mathcal{F}$  and every number in  $\mathcal{K}$  is algebraic over  $\mathcal{F}$ ,  $\mathcal{K}$  is said to be algebraic over  $\mathcal{F}$ .

#### THEOREM

*If  $\mathcal{K}$  is of degree  $n$  over  $\mathcal{F}$ ,  $\mathcal{K}$  is algebraic over  $\mathcal{F}$  and every number in  $\mathcal{K}$  is of degree  $n$  or less over  $\mathcal{F}$ .*

*Proof:* Since  $\mathcal{K}$  is of degree  $n$  over  $\mathcal{F}$ , by the lemma of §2 any  $n + 1$  numbers in  $\mathcal{K}$  are linearly dependent over  $\mathcal{F}$ . In particular, if  $\xi$  is in  $\mathcal{K}$ , then 1,  $\xi, \xi^2, \dots, \xi^n$  are in  $\mathcal{K}$  and are linearly dependent over  $\mathcal{F}$ . Hence  $a_0 + a_1 \xi + \dots + a_n \xi^n = 0$  where the  $a$ 's are in  $\mathcal{F}$  and are not all zero. Thus  $\xi$  is a root of a non-zero polynomial

with coefficients in  $\mathfrak{F}$  and of degree at most  $n$ , which proves the theorem.

### Exercises

- 1 Prove: A single number is linearly dependent over  $\mathfrak{F}$  if and only if it is zero.
- 2 If  $u$  and  $v$  are linearly dependent over  $\mathfrak{F}$  and  $u \neq 0$ , then  $v/u$  is in  $\mathfrak{F}$ , and conversely.
- 3 If among  $u_1, \dots, u_n$  there are fewer than  $n$  which are linearly dependent over  $\mathfrak{F}$ , then  $u_1, \dots, u_n$  are linearly dependent over  $\mathfrak{F}$ .
- 4 Show that each of the following sets are linearly independent over the given field:
  - a)  $3, \sqrt{2}, \sqrt{5}$ , rational field
  - b)  $1, \sqrt{2}, \sqrt[3]{2}$ , rational field
  - c)  $1, i, i + \sqrt{7}$ , rational field
  - d)  $1, \sqrt[3]{2}$ , field of numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are any rational numbers
- 5 Show that  $\sqrt{3}, \sqrt{2}, 1 + \sqrt{6}$  are linearly dependent over any field which contains  $\sqrt{3}$ .
- 6 Prove: If  $u_1, \dots, u_n$  are linearly independent over  $\mathfrak{F}$ , then  $v_i \triangleq c_{i1}u_1 + \dots + c_{in}u_n$  ( $i = 1, 2, \dots, n$ ) are linearly independent over  $\mathfrak{F}$  if the  $c$ 's are in  $\mathfrak{F}$  and  $c_{11}c_{22} \dots c_{nn} \neq 0$ .
- 7 Prove. If  $u_1, \dots, u_n$  is a basis for  $\mathcal{K}$  over  $\mathfrak{F}$ , then  $u_1, \dots, u_n$  are linearly independent over  $\mathfrak{F}$ .
- 8 Prove:  $\xi$  is algebraic over  $\mathfrak{F}$  if and only if there is a positive integer  $n$  such that  $1, \xi, \dots, \xi^n$  are linearly dependent over  $\mathfrak{F}$ .
- 9 Prove: The field of real numbers is not of finite degree over the field of rational numbers.
- 10 Prove:  $\mathcal{K}$  is of degree 1 over  $\mathfrak{F}$  if and only if it is identical with  $\mathfrak{F}$ .
- 11 Let  $\mathcal{K}$  be an extension of  $\mathfrak{F}$  and  $u_1, \dots, u_n$  numbers in  $\mathcal{K}$  such that every number in  $\mathcal{K}$  is expressible in the form  $c_1u_1 + \dots + c_ku_k$  with  $c_1, \dots, c_k$  in  $\mathfrak{F}$ . Let  $n$  be the maximum number of  $u_1, \dots, u_n$  which are linearly independent over  $\mathfrak{F}$ . Prove: If  $u_1, \dots, u_n$  are linearly independent over  $\mathfrak{F}$ , then  $u_1, \dots, u_n$  is a basis for  $\mathcal{K}$  over  $\mathfrak{F}$ .
- 12 Prove: If  $\mathcal{K}$  is an extension of  $\mathfrak{F}$  and any  $n+1$  numbers in  $\mathcal{K}$  are linearly dependent over  $\mathfrak{F}$ , then  $\mathcal{K}$  is of degree  $k \leq n$  over  $\mathfrak{F}$ .
- 13 Prove: If  $\mathcal{K}$  is of degree  $n$  over  $\mathfrak{F}$ , then any  $n$  numbers of  $\mathcal{K}$  which are linearly independent over  $\mathfrak{F}$  form a basis for  $\mathcal{K}$  over  $\mathfrak{F}$ .
- 14 Prove: If  $\mathcal{K} \supset \mathcal{L} \supset \mathfrak{F}$  and  $\mathcal{K}$  is algebraic over  $\mathfrak{F}$ , then  $\mathcal{K}$  is algebraic over  $\mathcal{L}$  and  $\mathcal{L}$  is algebraic over  $\mathfrak{F}$ .
- \*15 Prove: If  $u_1, \dots, u_n$  is a basis for  $\mathcal{K}$  over  $\mathcal{L}$  and  $v_1, \dots, v_m$  is a basis for  $\mathcal{L}$  over  $\mathfrak{F}$ , then the  $mn$  products  $u_iv_j$  are a basis for  $\mathcal{K}$  over  $\mathfrak{F}$ .

\*16 Prove: If  $\mathcal{K} \supset \mathcal{L} \supset \mathcal{F}$  and  $\mathcal{K}$  is of finite degree over  $\mathcal{F}$ , then  $\mathcal{K}$  is of finite degree over  $\mathcal{L}$  and  $\mathcal{L}$  is of finite degree over  $\mathcal{F}$ .

**4. Adjunction to a field** If  $\mathcal{F}$  is a field and  $S$  is a set of numbers, which may or may not belong to  $\mathcal{F}$ , there is at least one field which contains both  $\mathcal{F}$  and  $S$ , the field of all complex numbers. Let  $\mathcal{K}$  be the set of numbers common to all fields which contain both  $\mathcal{F}$  and  $S$ . If  $a$  and  $b$  are in  $\mathcal{K}$ , then  $a$  and  $b$  belong to all those fields; hence,  $a + b$ ,  $a - b$ ,  $ab$ , and  $a/b$  (if  $b \neq 0$ ) also belong to all the fields and, therefore, are in  $\mathcal{K}$ . Since every field contains the numbers 0 and 1 (ex. 2, §5, Ch. 2),  $\mathcal{K}$  does also. Hence  $\mathcal{K}$  contains at least two numbers. Thus,  $\mathcal{K}$  is a field.

From the definition of  $\mathcal{K}$  we see that it contains both  $\mathcal{F}$  and  $S$  and is contained in every field which contains both  $\mathcal{F}$  and  $S$ . In this sense it is the smallest field containing both  $\mathcal{F}$  and  $S$ . It is said to be obtained by adjoining  $S$  to  $\mathcal{F}$  and is denoted by  $\mathcal{F}(S)$ .

#### THEOREM

*If every number in  $S_1$  or  $S_2$  is in  $S$  and every number in  $S$  is in  $S_1$  or  $S_2$  (or both) and  $\mathcal{F}_1 = \mathcal{F}(S_1)$ , then  $\mathcal{F}_1(S_2) = \mathcal{F}(S)$ .*

In other words, to adjoin  $S$  to  $\mathcal{F}$  we may adjoin part of  $S$  to  $\mathcal{F}$  and then adjoin the remaining part of  $S$  to the result.

*Proof:*  $\mathcal{F}(S)$  contains  $\mathcal{F}$  and  $S$ . Therefore, it contains  $\mathcal{F}$  and  $S_1$ . Hence it contains  $\mathcal{F}_1$ . Since  $\mathcal{F}_1$  contains  $\mathcal{F}_1$  and  $S_2$ , it contains  $\mathcal{F}_1(S_2)$ .

$\mathcal{F}_1(S_2)$  contains  $\mathcal{F}_1$  and  $S_2$ . Hence it contains  $\mathcal{F}$ ,  $S_1$  and  $S_2$ . Therefore it contains  $\mathcal{F}$  and  $S$  and, consequently,  $\mathcal{F}(S)$ .

Since each of  $\mathcal{F}_1(S_2)$  and  $\mathcal{F}(S)$  contains the other, they are identical.

#### COROLLARY

*If  $\mathcal{F}_1 = \mathcal{F}(\xi_1)$ ,  $\mathcal{F}_2 = \mathcal{F}_1(\xi_2)$ ,  $\dots$ ,  $\mathcal{F}_n = \mathcal{F}_{n-1}(\xi_n)$ , then  $\mathcal{F}_n = \mathcal{F}(\xi_1, \xi_2, \dots, \xi_n)$ .*

In other words, the adjunction of  $n$  numbers to  $\mathcal{F}$  can be achieved by  $n$  successive adjunctions of single numbers.

*Proof:* This follows from the theorem by mathematical induction on  $n$ , by first adjoining  $\xi_1, \dots, \xi_{n-1}$  to  $\mathcal{F}$  and then adjoining  $\xi_n$  to the result.

*Example* If  $\mathfrak{F}$  is the field of rational numbers, describe the numbers of the field  $\mathfrak{F}(\sqrt{2}, \sqrt{3})$ .

Every field containing  $\mathfrak{F}$  and  $\sqrt{2}$  contains all the numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are rational. Since these numbers form a field (ex. 1(c), §5, (Ch. 2), they form the smallest field containing  $\mathfrak{F}$  and  $\sqrt{2}$ , i.e., they constitute  $\mathfrak{F}(\sqrt{2}) = \mathfrak{F}_1$ .

Similarly,  $\mathfrak{F}_1(\sqrt{3})$  consists of all the numbers of the form  $c + d\sqrt{3}$  where  $c$  and  $d$  belong to  $\mathfrak{F}_1$ .

Thus,  $\mathfrak{F}(\sqrt{2}, \sqrt{3})$  consists of all the numbers of the form  $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})\sqrt{3} = \alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}$  where  $\alpha, \beta, \gamma, \delta$  are rational.

## 5. Adjunction of algebraic numbers

### THEOREM

*If  $\xi$  is of degree  $n$  over  $\mathfrak{F}$ , then  $\mathfrak{F}(\xi)$  is of degree  $n$  over  $\mathfrak{F}$  with  $1, \xi, \xi^2, \dots, \xi^{n-1}$  as a basis.*

*Proof:* Since  $\mathfrak{F}(\xi)$  contains  $\mathfrak{F}$  and  $\xi$ , it contains every number of the form  $a_0 + a_1\xi + \dots + a_{n-1}\xi^{n-1}$  where  $a_0, a_1, \dots, a_{n-1}$  are in  $\mathfrak{F}$  (ex. 9, §5, (Ch. 2)). Therefore, if  $\mathcal{K}$  is the set of all numbers of this form,  $\mathcal{K}$  is contained in  $\mathfrak{F}(\xi)$ .

Letting  $a_1 = 1$  and  $a_i = 0$  for  $i \neq 1$ , we see that  $\mathcal{K}$  contains  $\xi$ . Letting  $a_i = 0$  for  $i \neq 0$ , we see that every number of  $\mathfrak{F}$  is in  $\mathcal{K}$ .

We shall show that  $\mathcal{K}$  is a field. Since  $\mathcal{K}$  contains both  $\mathfrak{F}$  and  $\xi$ , it will follow that  $\mathcal{K}$  contains  $\mathfrak{F}(\xi)$ . Since we already know that  $\mathcal{K}$  is contained in  $\mathfrak{F}(\xi)$ , this will show that  $\mathcal{K}$  and  $\mathfrak{F}(\xi)$  are identical.

$$\begin{aligned}\text{Let} \quad \alpha &= a_0 + a_1\xi + \dots + a_{n-1}\xi^{n-1} \\ \beta &= b_0 + b_1\xi + \dots + b_{n-1}\xi^{n-1}\end{aligned}$$

where the  $a$ 's and  $b$ 's are in  $\mathfrak{F}$ .

Obviously,  $\alpha + \beta$  and  $\alpha - \beta$  are expressible in the same form and, therefore, belong to  $\mathcal{K}$ .

To consider  $\alpha\beta$  and  $\alpha/\beta$ , let

$$\begin{aligned}f(x) &\equiv a_0 + a_1x + \dots + a_{n-1}x^{n-1} \\ g(x) &\equiv b_0 + b_1x + \dots + b_{n-1}x^{n-1}\end{aligned}$$

so that  $\alpha = f(\xi)$  and  $\beta = g(\xi)$ .

Let  $F(x)$  be the minimum polynomial of  $\xi$  over  $\mathfrak{F}$ . By the division algorithm (§6, Ch. 2),

$$f(x)g(x) \equiv Q(x)F(x) + (c_0 + c_1x + \cdots + c_{n-1}x^{n-1})$$

where the  $c$ 's are in  $\mathfrak{F}$ . Letting  $x = \xi$ ,

$$\begin{aligned}\alpha\beta = f(\xi)g(\xi) &= Q(\xi)F(\xi) + c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1} \\ &= c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}\end{aligned}$$

so that  $\alpha\beta$  has the required form and, therefore, is in  $\mathfrak{K}$ .

Suppose  $\beta = g(\xi) \neq 0$ .

Since  $F(x)$  is irreducible over  $\mathfrak{F}$ , the only polynomials with coefficients in  $\mathfrak{F}$  which are factors of  $F(x)$  are constants and  $cF(x)$  where  $c$  is in  $\mathfrak{F}$  (§11, Ch. 2). Since  $g(\xi) \neq 0$ , none of the latter is a factor of  $g(x)$ . Therefore, the only common factors of  $g(x)$  and  $F(x)$  with coefficients in  $\mathfrak{F}$  are constants. That is,  $g(x)$  and  $F(x)$  are relatively prime over  $\mathfrak{F}$  (§10, Ch. 2). It follows (§10, Ch. 2) that there are polynomials  $A(x)$  and  $B(x)$  with coefficients in  $\mathfrak{F}$  such that

$$A(x)g(x) + B(x)F(x) \equiv 1$$

Letting  $x = \xi$ , we have  $A(\xi)g(\xi) = 1$ , so that  $1/\beta = 1/g(\xi) = A(\xi)$ .

As above, by means of the division algorithm,  $f(\xi)A(\xi) = \alpha/\beta$  is in  $\mathfrak{K}$ . Thus  $\mathfrak{K}$  is a field, so that  $\mathfrak{K} = \mathfrak{F}(\xi)$ .

That  $1, \xi, \dots, \xi^{n-1}$  is a basis for  $\mathfrak{K}$  over  $\mathfrak{F}$  follows from the fact that the expression  $a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$  for a number in  $\mathfrak{K}$  is unique. For if  $a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} = b_0 + b_1\xi + \cdots + b_{n-1}\xi^{n-1}$ , where the  $a$ 's and  $b$ 's are in  $\mathfrak{F}$ , then  $(a_0 - b_0) + (a_1 - b_1)\xi + \cdots + (a_{n-1} - b_{n-1})\xi^{n-1} = 0$ . Since  $\xi$  is of degree  $n$  over  $\mathfrak{F}$ , this is possible only if all the  $a_i - b_i$  are zero.

This completes the proof of the theorem.

*Example* If  $\mathfrak{F}$  is the field of rational numbers, describe the numbers in  $\mathfrak{F}(\sqrt[3]{2})$ , where  $\sqrt[3]{2}$  is any cube root of 2.

$\sqrt[3]{2}$  is a root of  $x^3 - 2$ . This is irreducible over  $\mathfrak{F}$ . For if it were reducible it would have a linear factor with rational coefficients and, therefore, a rational root. But  $x^3 - 2$  has no rational root. Thus,  $\sqrt[3]{2}$  is of degree 3 over  $\mathfrak{F}$ . Hence  $\mathfrak{F}(\sqrt[3]{2})$  consists of all the numbers of the form  $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ , where  $a, b, c$  are rational.

## THEOREM

If  $\xi_1, \xi_2, \dots, \xi_k$  are of degrees  $n_1, n_2, \dots, n_k$  respectively over  $\mathfrak{F}$ , then  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k)$  is of degree  $m$  over  $\mathfrak{F}$ , where  $m \leq n_1 n_2 \dots n_k$ , and a basis for  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k)$  over  $\mathfrak{F}$  is included among the  $n_1 n_2 \dots n_k$  numbers  $\xi_1^{i_1} \xi_2^{i_2} \dots \xi_k^{i_k}$ , where  $i_1, i_2, \dots, i_k$  are non-negative integers not exceeding  $n_1 - 1, n_2 - 1, \dots, n_k - 1$  respectively.

*Proof:* By the preceding theorem, the desired result is true for  $k = 1$ . Proceeding by mathematical induction, suppose it true when there are  $k - 1$   $\xi$ 's.

We have  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k) = \mathfrak{F}'(\xi_k)$  where  $\mathfrak{F}' = \mathfrak{F}(\xi_1, \xi_2, \dots, \xi_{k-1})$  (§4). By the hypothesis of the induction,  $\mathfrak{F}'$  is of degree  $p$  over  $\mathfrak{F}$ , where  $p \leq n_1 n_2 \dots n_{k-1}$ , and a basis for  $\mathfrak{F}'$  over  $\mathfrak{F}$  is included among  $\xi_1^{i_1} \xi_2^{i_2} \dots \xi_{k-1}^{i_{k-1}}$  where  $0 \leq i_1 \leq n_1 - 1, 0 \leq i_2 \leq n_2 - 1, \dots, 0 \leq i_{k-1} \leq n_{k-1} - 1$ .

Since  $\xi_k$  is of degree  $n_k$  over  $\mathfrak{F}$ , it is a root of a polynomial of degree  $n_k$  with coefficients in  $\mathfrak{F}$ . These coefficients are also in  $\mathfrak{F}'$ , since  $\mathfrak{F}'$  contains  $\mathfrak{F}$ . Hence,  $\xi_k$  is of degree  $n$  over  $\mathfrak{F}'$ , where  $n \leq n_k$ .

By the preceding theorem,  $\mathfrak{F}'(\xi_k)$  is of degree  $n$  over  $\mathfrak{F}'$  with  $1, \xi_k, \xi_k^2, \dots, \xi_k^{n-1}$  as a basis over  $\mathfrak{F}'$ . By ex. 15, §3,  $\mathfrak{F}'(\xi_k)$  is of degree  $pn$  over  $\mathfrak{F}$  with a basis consisting of  $pn$  of the products  $\xi_1^{i_1} \xi_2^{i_2} \dots \xi_{k-1}^{i_{k-1}} \xi_k^{i_k}$ , where  $0 \leq i_1 \leq n_1 - 1, \dots, 0 \leq i_{k-1} \leq n_{k-1} - 1, 0 \leq i_k \leq n - 1 \leq n_k - 1$ .

Thus,  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k)$  is of degree  $pn \leq n_1 n_2 \dots n_{k-1} n_k$  over  $\mathfrak{F}$  with a basis of the form required.

By the principle of mathematical induction, the theorem is proved.

## COROLLARY

If  $\xi_1, \xi_2, \dots, \xi_k$  are algebraic over  $\mathfrak{F}$ , then  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k)$  is algebraic over  $\mathfrak{F}$ .

*Proof:* This follows from the theorem of §3, since  $\mathfrak{F}(\xi_1, \xi_2, \dots, \xi_k)$  is of finite degree over  $\mathfrak{F}$ .

*Remark* Since each of the  $\xi$ 's is in  $\mathfrak{F}(\xi_1, \dots, \xi_k)$ , every number expressible as a sum of numbers of the form  $a \xi_1^{i_1} \dots \xi_k^{i_k}$ , where  $a$  is in  $\mathfrak{F}$  and  $0 \leq i_1 \leq n_1 - 1, \dots, 0 \leq i_k \leq n_k - 1$ , is in  $\mathfrak{F}(\xi_1, \dots, \xi_k)$ . Furthermore, every number in  $\mathfrak{F}(\xi_1, \dots, \xi_k)$  is so



expressible since the  $\xi_1^i \cdots \xi_k^i$  include a basis for  $\mathfrak{F}(\xi_1, \dots, \xi_k)$  over  $\mathfrak{F}$ . Thus,  $\mathfrak{F}(\xi_1, \dots, \xi_k)$  consists of all the numbers expressible in this form.

*Example 1* If  $\mathfrak{F}$  is the field of rational numbers, describe the numbers of the field  $\mathfrak{F}(\sqrt{2}, \sqrt{3})$ . (We have already discussed this example in another way in §4.)

$\sqrt{2}$  and  $\sqrt{3}$  are roots of  $x^2 - 2$  and  $x^2 - 3$  respectively. Since each of these is irreducible over  $\mathfrak{F}$ ,  $\sqrt{2}$  and  $\sqrt{3}$  are of degree 2 over  $\mathfrak{F}$ . Thus,  $\mathfrak{F}(\sqrt{2}, \sqrt{3})$  consists of all the numbers of the form  $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$ , where  $a, b, c, d$  are rational.

*Example 2* Show that the set  $S$  of all numbers algebraic over  $\mathfrak{F}$  is a field.

Let  $a$  and  $b$  be algebraic over  $\mathfrak{F}$ . Then  $a + b$ ,  $a - b$ ,  $ab$ ,  $a/b$  (if  $b \neq 0$ ) are in  $\mathfrak{F}(a, b)$ . By the corollary above, every number in  $\mathfrak{F}(a, b)$  is algebraic over  $\mathfrak{F}$  and, therefore, is in  $S$ . Thus,  $S$  is a field.

### Exercises

- 1 Prove:  $\mathfrak{F}(S)$  consists of all the numbers obtainable by rational operations from numbers in  $\mathfrak{F}$  and  $S$ .
- 2 Prove: If every number in the set  $S$  belongs to  $\mathfrak{F}$ , then  $\mathfrak{F}(S)$  is identical with  $\mathfrak{F}$ , and conversely.
- 3 Prove: If  $u_1, u_2, \dots, u_n$  is a basis for  $\mathfrak{K}$  over  $\mathfrak{F}$ , then  $\mathfrak{K} = \mathfrak{F}(u_1, u_2, \dots, u_n)$ .
- 4 Prove: If  $\mathfrak{K} \supset \mathfrak{F}$  and  $\mathfrak{F}(\xi) \subset \mathfrak{K}$ , then  $\mathfrak{F}(\xi) = \mathfrak{K}(\xi)$ .
- 5 Prove: If  $\mathfrak{K}$  is of degree  $n$  over  $\mathfrak{F}$  and contains a number  $\xi$  of degree  $n$  over  $\mathfrak{F}$ , then  $\mathfrak{K} = \mathfrak{F}(\xi)$ .
- 6 Describe the numbers forming the following fields:
  - a)  $\mathfrak{F}(i)$ ,  $\mathfrak{F}$  the field of real numbers
  - b)  $\mathfrak{F}(1 + \sqrt{2})$ ,  $\mathfrak{F}$  the field of rational numbers
  - c)  $\mathfrak{F}(\sqrt{2}, \sqrt{6})$ ,  $\mathfrak{F}$  the field of rational numbers
  - d)  $\mathfrak{F}(1, \sqrt{7})$ ,  $\mathfrak{F}$  the field of rational numbers
  - e)  $\mathfrak{F}(\sqrt[3]{5}, i)$ ,  $\mathfrak{F}$  the field of real numbers
  - f)  $\mathfrak{F}(\sqrt[3]{4})$ ,  $\mathfrak{F}$  the field of rational numbers
  - g)  $\mathfrak{F}(\sqrt[3]{2})$   $\mathfrak{F}$  the field of numbers of the form  $a + b\sqrt{2}$  where  $a$  and  $b$  are rational (Use ex. 4(c), §1.)
  - h)  $\mathfrak{F}(\sqrt[3]{2}, \sqrt{5})$ ,  $\mathfrak{F}$  the field of rational numbers
- 7 Let  $\mathfrak{F}$  be the field of rational numbers and  $\xi$  a root of  $x^3 + 2x + 2$ . Express  $1 - 2\xi^4, 1/\xi, (1 - \xi)/(1 + \xi)$  in terms of the basis  $1, \xi, \xi^2$  of  $\mathfrak{F}(\xi)$  over  $\mathfrak{F}$ .

- 8 Let  $\mathcal{F}$  be the field of rational numbers and  $\xi$  a root of  $x^3 - 3x - 1$ . Express  $1/\xi^2$ ,  $3\xi^5$ ,  $\xi^4$  in terms of the basis  $1, \xi, \xi^2$  of  $\mathcal{F}(\xi)$  over  $\mathcal{F}$ .
- 9 Let  $\mathcal{F}$  be the field of rational numbers. Prove:
- $\mathcal{F}(1 + \sqrt{5})$  is identical with  $\mathcal{F}(3 - \sqrt{5})$
  - $\mathcal{F}(\sqrt{2}, \sqrt{6})$  is identical with  $\mathcal{F}(\sqrt{3}, \sqrt{2} - \sqrt{3})$ .
- 10 If  $a$  and  $b$  are roots of the same quadratic polynomial with coefficients in  $\mathcal{F}$ , show that  $\mathcal{F}(a)$  and  $\mathcal{F}(b)$  are identical.
- 11 Prove: If  $a, b, c, d$  are in  $\mathcal{F}$  and  $ad - bc \neq 0$ , and  $\beta = (a\alpha + b)/(c\alpha + d)$ , then  $\mathcal{F}(\alpha)$  and  $\mathcal{F}(\beta)$  are identical.
- 12 Prove: The field of all numbers algebraic over the rational field is not of finite degree over the rational field.
- 13 Prove: If  $S$  is an infinite set of numbers algebraic over  $\mathcal{F}$ ,  $\mathcal{F}(S)$  is algebraic over  $\mathcal{F}$ .
- 14 If  $\mathcal{K} \supset \mathcal{L} \supset \mathcal{F}$ ,  $\mathcal{K}$  algebraic over  $\mathcal{L}$  and  $\mathcal{L}$  algebraic over  $\mathcal{F}$ , then  $\mathcal{K}$  is algebraic over  $\mathcal{F}$ . [Hint: If  $\alpha$  is in  $\mathcal{K}$  and  $a_0x^n + \cdots + a_n$  is its minimum polynomial over  $\mathcal{L}$ , consider  $\mathcal{F}(\alpha, a_0, \dots, a_n)$ .]
- \*15 If  $\mathcal{K}$  is of degree  $n$  over  $\mathcal{F}$  and  $a$  in  $\mathcal{K}$  is of degree  $m$  over  $\mathcal{F}$ , then  $m$  is a divisor of  $n$ . [Hint:  $\mathcal{K} \supset \mathcal{F}(a) \supset \mathcal{F}$ .]
- 16 If  $\mathcal{F}$  is the field of rational numbers,  $p$  a positive prime integer,  $a$  a rational number with no rational  $p$ th root,  $\sqrt[p]{a}$  any  $p$ th root of  $a$ , then every number in  $\mathcal{F}(\sqrt[p]{a})$  is either rational or a root of a polynomial of degree  $p$  with rational coefficients irreducible over  $\mathcal{F}$ . (Hint: Use ex. 15 and ex. 15, §2, Ch. 5.)
- 17 If  $\mathcal{F}$  is the field of rational numbers, show (using ex. 15):
- $\sqrt[3]{2}$  is not in  $\mathcal{F}(\sqrt{2})$ .
  - $\sqrt{2}$  is not in  $\mathcal{F}(\sqrt[3]{2})$ .
  - $\sqrt[3]{2}$  is not in  $\mathcal{F}(\sqrt{2}, \sqrt{3}, \sqrt[3]{2}, \sqrt[3]{3})$ .

## 6. Adjunction of radicals

### THEOREM

If  $p$  is a positive prime integer,  $\omega \neq 1$  a  $p$ th root of 1,  $\mathcal{F}$  a field containing  $\omega$ ,  $\xi$  a  $p$ th root of a number in  $\mathcal{F}$ , then the degree of  $\xi$  over  $\mathcal{F}$  is 1 or  $p$ .

*Proof:* By hypothesis,  $\xi$  is a root of  $x^p - a$  where  $a$  is in  $\mathcal{F}$ .

Suppose  $a = b^p$  with  $b$  in  $\mathcal{F}$ . Then the roots of  $x^p - a$  are  $b, \omega b, \dots, \omega^{p-1}b$  (ex. 5, §13, Ch. 2). Since  $\mathcal{F}$  contains  $b$  and  $\omega$ ,  $\mathcal{F}$  contains all these roots. Hence, it contains  $\xi$ , which is one of these. Therefore,  $\xi$  is of degree 1 over  $\mathcal{F}$  (ex. 7, §1).

If  $a$  is not the  $p$ th power of any number in  $\mathfrak{F}$ ,  $x^p - a$  is irreducible over  $\mathfrak{F}$  (ex. 15, §2, Ch. 5). Hence,  $\xi$  is of degree  $p$  over  $\mathfrak{F}$ .

### THEOREM

*If  $p$  is a positive prime integer,  $\xi$  a  $p$ th root of a number in field  $\mathfrak{F}$ , then the degree of  $\xi$  over  $\mathfrak{F}$  is  $p$  or  $d$ , where  $d$  is a divisor of  $p - 1$ .*

*Proof:* Let  $d$  be the degree of  $\xi$  over  $\mathfrak{F}$ . Since  $\xi$  is a root of  $x^p - a$  with  $a$  in  $\mathfrak{F}$ ,  $d \leq p$ . If  $d = p$ , there is nothing more to be proved. Suppose, therefore,  $d < p$ .

Let  $\omega \neq 1$  be a  $p$ th root of 1,  $\mathfrak{F}' = \mathfrak{F}(\omega)$ . Let  $n$  be the degree of  $\omega$  over  $\mathfrak{F}$ . Then, by the first theorem of §5,  $\mathfrak{F}'$  is of degree  $n$  over  $\mathfrak{F}$ .

By the preceding theorem and the first theorem of §5, the degree of  $\mathfrak{F}'(\xi)$  over  $\mathfrak{F}'$  is 1 or  $p$ . Hence (ex. 15, §3), the degree of  $\mathfrak{F}'(\xi)$  over  $\mathfrak{F}$  is  $n$  or  $np$ . Since  $\xi$  is in  $\mathfrak{F}'(\xi)$ , the degree of  $\xi$  over  $\mathfrak{F}$  is a divisor of  $np$  (ex. 15, §5).

Since  $d < p$ ,  $d$  and  $p$  are relatively prime. Therefore (ex. 9, §10, Ch. 2, for integers),  $d$  is a divisor of  $n$ .

Thus, the theorem will be proved when we show that  $n$  is a factor of  $p - 1$ . This we do in the following:

### THEOREM

*If  $p$  is a positive prime integer,  $\omega \neq 1$  a  $p$ th root of 1,  $\mathfrak{F}$  any field, then the degree of  $\omega$  over  $\mathfrak{F}$  is a divisor of  $p - 1$ .*

*Proof:* If  $x^p - 1 \equiv (x - 1)f(x)$ , then  $f(x) \equiv x^{p-1} + x^{p-2} + \cdots + x + 1$  and  $\omega$  is a root of  $f(x)$ . If  $f(x) \equiv g_1(x)g_2(x) \cdots g_r(x)$  is the factorization of  $f(x)$  into polynomials prime over  $\mathfrak{F}$  with leading coefficients 1, then one of the factors is the minimum polynomial of  $\omega$  over  $\mathfrak{F}$ .

Let  $n$  be the greatest of the degrees of the  $g_i(x)$  and, to be specific, suppose  $g_1(x)$  of degree  $n$ .

If  $\alpha$  is a root of  $g_1(x)$ , then  $\alpha \neq 1$  and  $\alpha, \alpha^2, \cdots, \alpha^{p-1}$  are distinct and are all the roots of  $f(x)$  (ex. 5, §13, Ch. 2).

Suppose  $\alpha^k$ ,  $1 < k \leq p - 1$ , a root of  $g_2(x)$ . Then  $g_2(x^k)$  has coefficients in  $\mathfrak{F}$  and a root  $\alpha$  in common with  $g_1(x)$ . Hence (first theorem, §1, Ch. 5),  $g_2(x^k) \equiv g_1(x)h(x)$ .

If  $\lambda$  is any root of  $g_1(x)$ , then  $g_2(\lambda^k) = g_1(\lambda)h(\lambda) = 0$ , so that  $\lambda^k$  is a root of  $g_2(x)$ .

If  $\lambda_1, \lambda_2$  are distinct roots of  $g_1(x)$ , then  $\lambda_1^k, \lambda_2^k$  are distinct roots of  $g_2(x)$ . For,  $(\lambda_1/\lambda_2)^p = 1$ , so that  $\lambda_1/\lambda_2$ , which is different from 1, is a  $p$ th root of 1. Hence  $\lambda_1/\lambda_2, (\lambda_1/\lambda_2)^2, \dots, (\lambda_1/\lambda_2)^{p-1}$  are all the roots of  $f(x)$ . Therefore,  $(\lambda_1/\lambda_2)^k \neq 1$ , since 1 is not a root of  $f(x)$ .

Thus, if  $\lambda_1, \lambda_2, \dots, \lambda_n$  are the (necessarily distinct) roots of  $g_1(x)$ , then  $\lambda_1^k, \lambda_2^k, \dots, \lambda_n^k$  are distinct roots of  $g_2(x)$ . Hence, the degree of  $g_2(x)$  is at least  $n$ . Since the degree of  $g_2(x)$  does not exceed  $n$ , its degree is exactly  $n$ .

Similarly, every  $g_i(x)$  is of degree  $n$ . Hence,  $p - 1 = rn$ , and the theorem is proved.

For use in §7, we establish:

### COROLLARY

*If  $p_1, p_2, \dots, p_k$  are distinct positive prime integers,  $\omega_i \neq 1$  a  $p_i$ th root of 1 ( $i = 1, 2, \dots, k$ ),  $\mathfrak{F}$  any field, then the degree of  $\mathfrak{F}(\omega_1, \dots, \omega_k)$  over  $\mathfrak{F}$  is  $d_1 d_2 \dots d_k$ , where  $d_i$  is a divisor of  $p_i - 1$ .*

*Proof:* For  $k = 1$  this follows immediately from the theorem (using the first theorem, §5). Proceeding by mathematical induction, suppose it true for  $\mathfrak{F}(\omega_1, \dots, \omega_k)$ .

By the theorem, the degree of  $\mathfrak{F}(\omega_1, \dots, \omega_k, \omega_{k+1}) = \mathfrak{F}'(\omega_{k+1})$ , where  $\mathfrak{F}' = \mathfrak{F}(\omega_1, \dots, \omega_k)$ , over  $\mathfrak{F}'$  is  $d_{k+1}$ , a divisor of  $p_{k+1} - 1$ . By the hypothesis of the induction, the degree of  $\mathfrak{F}'$  over  $\mathfrak{F}$  is  $d_1 d_2 \dots d_k$ . The desired result now follows by using ex. 15, §3.

*Example* Let  $\sqrt[3]{2}$  be the real cube root of 2,  $\omega \neq 1$  a cube root of 1,  $\xi = \omega \sqrt[3]{2}$ . Then  $\xi$  is a root of  $x^3 - 2$ .

If  $\mathfrak{F}$  is the field of rational numbers,  $x^3 - 2$  is irreducible over  $\mathfrak{F}$ , so that  $\xi$  is of degree 3 over  $\mathfrak{F}$ .

If  $\mathfrak{F}$  is the field obtained by adjoining  $\sqrt[3]{2}$  to the rational field, then  $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$  is reducible over  $\mathfrak{F}$ . All the numbers in  $\mathfrak{F}$  are real and  $\xi$  is not. Hence,  $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ , of which  $\xi$  is a root, has no linear factor with coefficients in  $\mathfrak{F}$ ; hence, it is irreducible over  $\mathfrak{F}$ . Thus,  $\xi$  is of degree 2 over  $\mathfrak{F}$ .

**7. Expressibility by radicals** A number  $r$  is said to be obtainable by radicals from the numbers  $a_1, a_2, \dots$  (finite in number or infinitely many) if there exists a sequence  $b_1, b_2, \dots, b_n$  with

$b_n = r$  and such that every  $b_i$  is either one of the  $a$ 's or equals  $b_j + b_k$ ,  $b_j b_k$ ,  $b_j - b_k$ , or  $b_j/b_k$ , or a root of  $b_j$  of some index, where  $j$  and  $k$  are less than  $i$ .

In any such sequence we may always suppose that every radical is of prime index. For if  $\sqrt[m]{c}$  appears and  $m = p_1 p_2 \cdots p_k$ , where the  $p$ 's are positive prime integers (not necessarily distinct), then  $\sqrt[m]{c}$  can be replaced by the sequence  $c_1, c_2, \cdots, c_{k+1}$  where  $c_1 = c$ ,  $c_2 = \sqrt[p_1]{c_1}$ ,  $c_3 = \sqrt[p_2]{c_2}$ ,  $\cdots$ ,  $c_{k+1} = \sqrt[p_k]{c_k} = \sqrt[m]{c}$ , each radical being properly chosen.

### THEOREM

Suppose  $r$  obtainable from  $a_1, a_2, \cdots$  by radicals of indices  $p_1, p_2, \cdots, p_k$ , where the  $p$ 's are distinct primes (although radicals with these indices may appear more than once in the sequence  $b_1, b_2, \cdots, b_n$ ). Let  $\omega_i \neq 1$  ( $i = 1, 2, \cdots, k$ ) be a  $p_i$ th root of 1. Let  $\mathfrak{F}$  be a field containing the  $a$ 's and  $\omega_1, \omega_2, \cdots, \omega_k$ . Then the degree of  $r$  over  $\mathfrak{F}$  is  $p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ , where  $i_1, i_2, \cdots, i_k$  are non-negative integers.

*Proof:* Let  $\mathfrak{F}_i = \mathfrak{F}(b_1, \cdots, b_i)$  ( $i = 1, 2, \cdots, n$ ). We show that the degree of every  $\mathfrak{F}_i$  over  $\mathfrak{F}$  has the form  $p_1^{i_1} \cdots p_k^{i_k}$ .

For  $i = 1$  this is obvious. For  $b_1$  is one of the  $a$ 's, so that  $\mathfrak{F}(b_1)$  is of degree 1 over  $\mathfrak{F}$  (ex. 7, §1).

Proceeding by mathematical induction, suppose the degree of  $\mathfrak{F}_{i-1}$  over  $\mathfrak{F}$  is  $p_1^{r_1} \cdots p_k^{r_k}$  where the  $r$ 's are non-negative integers.

If  $b_i$  is  $b_j + b_k$  or  $b_j - b_k$  or  $b_j b_k$  or  $b_j/b_k$  or  $b_j$ ,  $j$  and  $k$  less than  $i$ , then  $b_i$  is in  $\mathfrak{F}_{i-1}$ . Hence,  $\mathfrak{F}_i$  is of degree 1 over  $\mathfrak{F}_{i-1}$ . Therefore,  $\mathfrak{F}_i$  is of degree  $p_1^{r_1} \cdots p_k^{r_k}$  over  $\mathfrak{F}$  (ex. 15, §3).

If  $b_i$  is a  $p$ th root of  $b_j$ , where  $j \leq i-1$ , then by the first theorem of §6,  $b_i$  is of degree 1 or  $p$  over  $\mathfrak{F}_{i-1}$ . Hence (ex. 15, §3), the degree of  $\mathfrak{F}_i$  over  $\mathfrak{F}$  is  $p_1^{r_1} \cdots p_k^{r_k}$  or  $p_1^{r_1} \cdots p_k^{r_k} p$ , which establishes the desired result for  $\mathfrak{F}_i$ .

Now,  $r$  is in  $\mathfrak{F}_n$ . Hence its degree over  $\mathfrak{F}$  is a factor of the degree of  $\mathfrak{F}_n$  over  $\mathfrak{F}$  (ex. 15, §5). Since every factor of  $p_1^{r_1} \cdots p_k^{r_k}$  has this same form (by the unique factorization theorem for integers), the theorem is proved.

### THEOREM

If  $r$  is obtainable from  $a_1, a_2, \cdots$  by radicals of indices  $p_1, \cdots, p_k$ , where the  $p$ 's are distinct primes, and  $\mathfrak{F}$  is a field containing the

$a$ 's, the degree of  $r$  over  $\mathfrak{F}$  is  $d_1 \cdots d_k p_1^{i_1} \cdots p_k^{i_k}$ , where the  $i$ 's are non-negative integers, and  $d_1, \cdots, d_k$  are divisors of  $p_1 - 1, \cdots, p_k - 1$ .

*Proof:* Let  $\omega_i \neq 1$  ( $i = 1, \cdots, k$ ) be a  $p_i$ th root of 1,  $\mathfrak{F}' = \mathfrak{F}(\omega_1, \cdots, \omega_k)$ . By the corollary in §6, the degree of  $\mathfrak{F}'$  over  $\mathfrak{F}$  is  $d_1 \cdots d_k$ , where  $d_i$  is a divisor of  $p_i - 1$ .

By the preceding theorem the degree of  $r$  over  $\mathfrak{F}'$  is  $p_1^{i_1} \cdots p_k^{i_k}$ . Therefore (first theorem, and ex. 15, §3), the degree of  $\mathfrak{F}'(r)$  over  $\mathfrak{F}$  is  $d_1 \cdots d_k p_1^{i_1} \cdots p_k^{i_k}$ . Since  $r$  is in  $\mathfrak{F}'(r)$ , the degree of  $r$  over  $\mathfrak{F}$  is a factor of  $d_1 \cdots d_k p_1^{i_1} \cdots p_k^{i_k}$  (ex. 15, §5). It follows (ex. 6, §13, Ch. 2) that the degree of  $r$  over  $\mathfrak{F}$  is  $d'_1 \cdots d'_k p_1^{i_1} \cdots p_k^{i_k}$ , where  $d'_i$  is a factor of  $d_i$ , and the theorem is proved.

### COROLLARY

*If  $r$  is obtainable from numbers in a field  $\mathfrak{F}$  by rational operations and extractions of square roots, the degree of  $r$  over  $\mathfrak{F}$  is a non-negative integral power of 2.*

*Proof:* In the theorem,  $k = 1$ ,  $p_1 = 2$ ,  $d_1 = 1$ .

In particular, suppose  $r$  is obtainable from numbers in  $\mathfrak{F}$  by rational operations and extractions of square roots and is a root of a cubic polynomial  $f(x)$  with coefficients in  $\mathfrak{F}$ . Let  $g(x)$  be the minimum polynomial of  $r$  over  $\mathfrak{F}$ . Then, by the corollary,  $g(x)$  is of degree 1 or 2. But  $g(x)$  is a factor of  $f(x)$  (§1). Hence,  $f(x)$  has a linear factor with coefficients in  $\mathfrak{F}$  and, therefore, a root in  $\mathfrak{F}$ . This proves once again the second part of the theorem in §5, Ch. 9.

An equation  $f(x) = 0$  is said to be solvable by radicals if all its roots are obtainable by radicals from the coefficients of  $f(x)$ . Not every equation of degree greater than 4 is solvable by radicals. In fact, some equations have no root obtainable from the coefficients by radicals. Unfortunately, we cannot go into the proofs (which will be found in the Galois theory of equations).

*Example* If  $f(x)$  of degree  $n > 1$  is irreducible over the field  $\mathfrak{F}$  and  $n$  is divisible by a prime other than 2, 3, or 7, then  $f(x)$  has no root obtainable from numbers in  $\mathfrak{F}$  by rational operations and extractions of square roots, cube roots and seventh roots.

If  $f(x)$  has such a root  $r$ , then the degree of  $r$  over  $\mathfrak{F}$  is  $d_1 d_2 d_3 2^i 3^j 7^k$ , where  $d_1, d_2, d_3$  are factors of 1, 2, 6 respectively and  $i, j, k$  are non-negative integers. Every such integer has the form  $2^a 3^b 7^c$ .

Since  $f(x)$  is irreducible, the degree of  $r$  over  $\mathfrak{F}$  is  $n$ . Hence,  $n$  must have this form.

### Exercises

- 1 Let  $f(x)$  be irreducible over  $\mathfrak{F}$  and of degree  $n$ . Show that it has no root obtainable from numbers in  $\mathfrak{F}$  by rational operations and extractions of:
  - a) cube roots if  $n = 4$
  - b) square roots and fifth roots if  $n = 6$
  - c) square roots, cube roots and fifth roots if  $n = 7$
  - d)  $p$ th roots, if  $p$  is an odd prime integer not of the form  $8k + 1$ , if  $n = 8$
  - e) square roots, cube roots, seventh roots and eleventh roots, if  $n$  is not of the form  $2^a 3^b 5^c 7^d 11^e$  where  $c \leq 1$
  - f) roots of indices  $p_1, p_2, \dots, p_k$ , where  $p_1, p_2, \dots, p_k$  are the first  $k$  primes in order of magnitude, if  $n$  is divisible by a prime greater than  $p_k$ .
- 2 If  $\cos A$  is rational then it is impossible with ruler and compasses to construct
  - a)  $A/5$  if  $16x^5 - 20x^3 + 5x - \cos A$  is irreducible over the rational field
  - b)  $A/7$  if  $64x^7 - 112x^5 + 56x^3 - 7x - \cos A$  is irreducible over the rational field.

(Remark: It can be shown that if  $\cos A = 5m/n$ , where neither  $m$  nor  $n$  is divisible by 5, then (a) is irreducible; if  $\cos A = 7m/n$ , where neither  $m$  nor  $n$  is divisible by 7, then (b) is irreducible.)

## SYMMETRIC POLYNOMIALS

**1. Polynomials in several variables** If  $x$ ,  $y$  and  $w$  are variables and to each ordered pair of values  $(x, y)$  there corresponds in some prescribed manner a value of  $w$ , then  $w$  is said to be a (one-valued) function of  $x$  and  $y$ , and we write  $w \equiv f(x, y)$  (or some other similar symbol).

This same symbol is used to denote the value of  $w$  which corresponds to  $(x, y)$ . When the variables are understood we frequently write  $f$  instead of  $f(x, y)$ .

If  $x$  and  $y$  denote any complex numbers and if there exist a non-negative integer  $m$  and complex numbers  $a_{ij}$  such that

$$(1) \quad f(x, y) \equiv a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 \\ + \cdots + a_{m0}x^m + a_{m-1,1}x^{m-1}y + \cdots + a_{1,m-1}xy^{m-1} + a_{0m}y^m,$$

then  $f(x, y)$  is called a polynomial in  $x$  and  $y$ .

The expression (1) can be written compactly as

$$\sum_{i+j=0}^m a_{ij}x^iy^j$$

This denotes the sum of all terms  $a_{ij}x^iy^j$  where  $i$  and  $j$  take on all non-negative integral values subject to  $0 \leq i + j \leq m$  (with the understanding that  $x^0$  or  $y^0$  is 1). In this notation each of the numbers  $a_{ij}$  has two subscripts which indicate the powers of  $x$  and  $y$  that the number multiplies. The first subscript shows the power of  $x$  and the second the power of  $y$ . For example, the number which multiplies  $x^7y^9$  is  $a_{7,9}$ .

We can, in a similar way, define a polynomial in any number of variables  $x_1, x_2, \dots, x_n$  as a function of these variables which can be expressed in the form



$$(2) \quad \sum_{i_1 + i_2 + \cdots + i_n = 0}^m a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

where the  $a$ 's are complex numbers and  $\Sigma$  denotes the sum of all the indicated products, the  $i$ 's being any non-negative integers subject to the condition  $0 \leq i_1 + i_2 + \cdots + i_n \leq m$ .

Each of the  $a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$  is called a term of the polynomial;  $a_{i_1 i_2 \cdots i_n}$  is the coefficient of the term;  $i_1 + i_2 + \cdots + i_n$  is the degree of the term and  $i_j$  its degree in  $x_j$ .

If  $f$  is a polynomial in  $x_1, x_2, \cdots, x_n$  for which there is an expression (2) such that

- (a) No term of degree greater than  $m$  has a non-zero coefficient
  - (b) At least one term of degree  $m$  has a non-zero coefficient,
- then  $f$  is said to be of degree  $m$ .

A polynomial of degree zero is called a constant polynomial (or, briefly, a constant); of degree 1, linear; of degree 2, quadratic etc.

We cannot speak of *the* degree of a polynomial until we have shown that all expressions of the form (2) for a given polynomial are the same, i.e., that the coefficients of the terms involving like powers of the  $x$ 's are the same in all such expressions.

If  $f$  and  $g$  are polynomials in  $x_1, x_2, \cdots, x_n$  with the same values for all sets of values ( $x_1, \cdots, x_n$ ), then they are identical polynomials, and we write  $f = g$ .

The polynomial  $f(x_1, x_2, \cdots, x_n)$  which vanishes identically, i.e., which equals zero for all values of the  $x$ 's, is called the zero polynomial.

### Exercises

- 1 Prove: The number of terms of degree  $i$  in the expression (1) is  $i + 1$ ; the total number of terms is  $\frac{1}{2}(m + 1)(m + 2)$ .
- 2 Prove: A polynomial  $f(x, y, z)$  can be expressed in the form  $f_0(x, y) + f_1(x, y)z + \cdots + f_p(x, y)z^p$  where each of the  $f(x, y)$  is a polynomial in  $x$  and  $y$ . Generalize to any number of variables.
- 3 Prove: If  $f$  and  $g$  are polynomials in  $x_1, x_2, \cdots, x_n$ , then  $f + g, f - g$  and  $fg$  are polynomials in  $x_1, x_2, \cdots, x_n$ .
- 4 Criticize the statement:  $(x - 1)/y$  is a polynomial in  $x$  and  $y$  for all values of  $x$  and  $y$  for which  $y \neq 0$ .

**5** Prove: If  $f(x, y)$  is a polynomial in  $x$  and  $y$ , and  $g(x)$  is a polynomial in  $x$  such that  $f(x, g(x)) \equiv 0$ , then  $f(x, y) \equiv [y - g(x)]h(x, y)$ , where  $h(x, y)$  is a polynomial in  $x$  and  $y$ .

**2. Uniqueness of representation** We have seen that a polynomial in one variable cannot vanish for infinitely many values of the variable unless it vanishes identically (§4, Ch. 2). A polynomial in more than one variable, however, may vanish for infinitely many sets of values of the variables without vanishing identically (for example,  $x - y$ ). In many respects, however, polynomials in several variables behave like polynomials in one variable.

### THEOREM

*A polynomial in  $x_1, x_2, \dots, x_n$  represented by the expression (2) of §1 vanishes identically if and only if all the coefficients are zero.*

*Proof:* Obviously, if all the coefficients are zero then the polynomial vanishes identically.

We prove the converse by mathematical induction on  $n$ .

For  $n = 1$  the expression (2) of §1 is a polynomial in one variable for which the desired result has already been established (§4, Ch. 2). Hence, suppose it true whenever there are  $k$  or fewer variables. Let  $n = k + 1$  in (2) and suppose the polynomial vanishes identically.

For simplicity in the proof let  $k + 1 = 3$  and denote the variables by  $x, y, z$ . (The proof, however, is perfectly general). Then

$$f(x, y, z) \equiv \sum_{i+j+k=0}^m a_{ijl} x^i y^j z^k$$

Grouping the terms according to the powers of  $z$ ,

$$\begin{aligned} f(x, y, z) &\equiv \left( \sum_{i+j=0}^m a_{ij0} x^i y^j \right) + \left( \sum_{i+j=0}^{m-1} a_{ij1} x^i y^j \right) z \\ &\quad + \left( \sum_{i+j=0}^{m-2} a_{ij2} x^i y^j \right) z^2 + \cdots + \left( \sum_{i+j=0}^0 a_{ijm} x^i y^j \right) z^m \end{aligned}$$

This is of the form

$$f(x, y, z) \equiv g_0(x, y) + g_1(x, y)z + \cdots + g_m(x, y)z^m$$

where each of the  $g_i(x, y)$  is a polynomial in  $x$  and  $y$ . The coefficients in the  $g_i(x, y)$  are the coefficients in  $f(x, y, z)$ .

Let  $(a, b)$  be any set of values of  $(x, y)$ . Then

$$f(a, b, z) = g_0(a, b) + g_1(a, b)z + \cdots + g_m(a, b)z^m$$

is a polynomial in  $z$ .

By hypothesis,  $f(x, y, z)$  vanishes for all values of  $x, y, z$ . Therefore,  $f(a, b, z)$  vanishes for all values of  $z$ . Hence (§4, Ch. 2), all the coefficients of the powers of  $z$  in this polynomial are zero. Thus,  $g_i(a, b) = 0$  for  $i = 0, 1, \dots, m$ .

Since this is true no matter what the numbers  $a$  and  $b$  may be,  $g_i(x, y) = 0$ . Hence, by the hypothesis of the induction, all the coefficients in all the  $g_i(x, y)$  are zero.

Thus, all the coefficients in  $f(x, y, z)$  are zero, so that the desired result holds for  $n = k + 1$ .

By the principle of mathematical induction, the theorem is proved.

According to the theorem, if a polynomial vanishes identically there is no way of expressing it in the form (2) with a non-zero coefficient. Therefore, the zero polynomial has no degree.

On the other hand, if a polynomial does not vanish identically an expression for it in the form (2) must have at least one non-zero coefficient. Every such polynomial, therefore, has some degree. We show now that the degree is unique by showing that there is essentially only one way of expressing a polynomial in the form (2).

### THEOREM

If

$$\sum_{i_1+i_2+\cdots+i_n=0}^m a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \equiv \sum_{j_1+j_2+\cdots+j_n=0}^{m'} b_{j_1 j_2 \cdots j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

where  $m' \geq m$ , then  $b_{j_1 j_2 \cdots j_n} = 0$

for  $j_1 + j_2 + \cdots + j_n > m$

and  $b_{j_1 j_2 \cdots j_n} = a_{j_1 j_2 \cdots j_n}$

for  $0 \leq j_1 + j_2 + \cdots + j_n \leq m$ .

*Proof:* The difference of the two given expressions is a polynomial in  $x_1, x_2, \dots, x_n$  which vanishes for all values of  $x_1, x_2,$

$\dots, x_n$ . Hence

$$\sum_{j_1+j_2+\dots+j_n=0}^m (b_{j_1j_2\dots j_n} - a_{j_1j_2\dots j_n})x_1^{j_1}x_2^{j_2}\dots x_n^{j_n} \\ + \sum_{j_1+j_2+\dots+j_n=m+1}^{m'} b_{j_1j_2\dots j_n}x_1^{j_1}x_2^{j_2}\dots x_n^{j_n} \equiv 0$$

(If  $m' = m$ , the second part is missing.)

The desired result now follows by applying the previous theorem.

### COROLLARY

*If a polynomial in  $x_1, x_2, \dots, x_n$  does not vanish identically, its degree is unique.*

Note: Throughout the remainder of the chapter all symbols for functions denote polynomials.

### Exercises

- \*1 Prove:  $f(x, y, z)$  can be expressed uniquely in the form  $f_0(x, y) + f_1(x, y)z + \dots + f_p(x, y)z^p$ . Generalize to polynomials in any number of variables.
- 2 A polynomial is said to be homogeneous if it vanishes identically or if all terms with non-zero coefficients have the same degree. (For example,  $3x^2 + yz$  is homogeneous of degree 2 in  $x, y, z$ .) Prove: If  $f(x_1, x_2, \dots, x_n) \not\equiv 0$  it can be expressed uniquely in the form  $f_1 + f_2 + \dots + f_p$  where each  $f$  is a non-zero polynomial homogeneous in  $x_1, x_2, \dots, x_n$  and all have different degrees.
- 3  $f(x_1, x_2, \dots, x_n)$  is said to be of degree  $m$  in  $x_1$  if it has a term  $a_{i_1i_2\dots i_n}x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$  where  $i_1 = m$  with a non-zero coefficient and no term where  $i_1 > m$  with a non-zero coefficient. (For example,  $x^2 - 3x^2yz + 4xyz^3 + z$  is of degree 2 in  $x$ , 1 in  $y$  and 3 in  $z$ .) Prove: The degree of a polynomial in each variable is unique.
- 4 Prove:  $f(x_1, x_2, \dots, x_n)$  is of degree  $m$  in  $x_n$  if and only if it can be expressed in the form  $f_0(x_1, x_2, \dots, x_{n-1}) + f_1(x_1, x_2, \dots, x_{n-1})x_n + \dots + f_m(x_1, x_2, \dots, x_{n-1})x_n^m$  where  $f_m \not\equiv 0$ .
- 5 Prove: If  $f(x_1, x_2, \dots, x_n) \not\equiv 0$  there are infinitely many sets of values  $(a_1, a_2, \dots, a_n)$  such that  $f(a_1, a_2, \dots, a_n) \neq 0$ .
- 6 Prove: If  $n > 1$  and  $f(x_1, x_2, \dots, x_n)$  is not a constant, there are infinitely many sets of values  $(a_1, a_2, \dots, a_n)$  such that  $f(a_1, a_2, \dots, a_n) = 0$ .

- 7 Prove: If  $f(x_1, x_2, \dots, x_n)$  is a polynomial in  $x_1, x_2, \dots, x_n$  and  $g_i(y_1, y_2, \dots, y_p)$  ( $i = 1, 2, \dots, n$ ) are polynomials in  $y_1, y_2, \dots, y_p$ , then  $f(g_1, g_2, \dots, g_n)$  is a polynomial in  $y_1, y_2, \dots, y_p$ .
- 8 If  $f(x)$  and  $g(y)$  are polynomials in  $x$ , there exists a polynomial  $h(x, y)$  such that  $f(x)g(y) - f(y)g(x) = (x - y)h(x, y)$ .
- 9 Prove: If  $f(x, y)$  vanishes for all real values of  $x$  and  $y$ , then it vanishes identically.

**3. Products of polynomials** If  $f$  and  $g$  are polynomials in  $x_1, x_2, \dots, x_n$ , evidently their sum or difference is a polynomial in  $x_1, x_2, \dots, x_n$  which is identically zero or of degree not greater than the degree of  $f$  or  $g$ . If  $f$  and  $g$  have different degrees, the degree of the sum or difference is the larger of the two.

If  $f$  and  $g$  are non-zero polynomials in the one variable  $x$ , it is easy to see that the degree of their product is the sum of their degrees. For, the coefficient of the highest power of  $x$  in the product is the product of the coefficients of the highest powers of  $x$  in  $f$  and  $g$ .

If  $f$  and  $g$  are polynomials in more than one variable, obviously the degree of  $fg$ , if any, does not exceed the sum of the degrees of  $f$  and  $g$ . But it is not obvious exactly what the degree is, since many like terms may have to be combined in order to find the coefficients of the terms of highest degree. However it is still true, as we shall prove, that the degree of  $fg$  is the sum of the degrees of  $f$  and  $g$ .

We first prove:

#### THEOREM

If  $f(x_1, \dots, x_n)g(x_1, \dots, x_n) \equiv 0$ , then  $f \equiv 0$  or  $g \equiv 0$ .

*Proof:* For  $n = 1$  the desired result has already been established (cancellation law for polynomials in one variable, §1, Ch. 2). Proceeding by mathematical induction, suppose it true for  $n = k$ . Let  $n = k + 1$ .

If  $f \not\equiv 0$  and  $g \not\equiv 0$ , then

$$\begin{aligned} f(x_1, \dots, x_k, x_{k+1}) &= f_0(x_1, \dots, x_k) + f_1(x_1, \dots, x_k)x_{k+1} \\ &\quad + \dots + f_p(x_1, \dots, x_k)x_{k+1}^p \\ g(x_1, \dots, x_k, x_{k+1}) &= g_0(x_1, \dots, x_k) + g_1(x_1, \dots, x_k)x_{k+1} \\ &\quad + \dots + g_q(x_1, \dots, x_k)x_{k+1}^q \end{aligned}$$

where  $p \geq 0, q \geq 0, f_p(x_1, \dots, x_k) \not\equiv 0, g_q(x_1, \dots, x_k) \not\equiv 0$ .

If  $h \equiv fg$ , by direct multiplication

$$h(x_1, \dots, x_k, x_{k+1}) \equiv f_p(x_1, \dots, x_k)g_q(x_1, \dots, x_k)x_{k+1}^p + h_1(x_1, \dots, x_k)x_{k+1}^{p+q-1} + \dots + h_{p+q}(x_1, \dots, x_k)$$

where  $h_1, \dots, h_{p+q}$  are polynomials in  $x_1, \dots, x_k$ .

Let  $a_1, \dots, a_k$  be any values of  $x_1, \dots, x_k$ . Since  $h(x_1, \dots, x_k, x_{k+1}) \equiv 0$  by hypothesis,  $h(a_1, \dots, a_k, x_{k+1}) = 0$  for all values of  $x_{k+1}$ . It follows from the theorem for  $n = 1$  that the coefficients of the powers of  $x_{k+1}$  in  $h(a_1, \dots, a_k, x_{k+1})$  are zero. Therefore, in particular,  $f_p(a_1, \dots, a_k)g_q(a_1, \dots, a_k) = 0$ .

Since this is true no matter what the numbers  $a_1, \dots, a_k$  may be,  $f_p(x_1, \dots, x_k)g_q(x_1, \dots, x_k) \equiv 0$ . Therefore, by the hypothesis of the induction,  $f_p(x_1, \dots, x_k) = 0$  or  $g_q(x_1, \dots, x_k) \equiv 0$ , which contradicts the assumption  $f \not\equiv 0$  and  $g \not\equiv 0$ .

Thus,  $f \equiv 0$  or  $g \equiv 0$ , and the theorem is established.

#### COROLLARY

If  $fg_1 \equiv fg_2$  and  $f \not\equiv 0$ , then  $g_1 \equiv g_2$ .

*Proof:* From the hypothesis,  $f(q_1 - g_2) = 0$ . Since  $f \not\equiv 0$ , it follows from the theorem that  $q_1 - g_2 = 0$ .

#### THEOREM

If  $f(x_1, \dots, x_n)$  and  $g(x_1, \dots, x_n)$  are of degrees  $p$  and  $q$  respectively, then  $fg$  is of degree  $p + q$ .

*Proof:* Suppose first that  $f$  and  $g$  are homogeneous polynomials. Then we may write  $f \equiv \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ , where  $i_1 + \dots + i_n = p$  for every term, and  $g \equiv \sum b_{j_1 \dots j_n} x_1^{j_1} \dots x_n^{j_n}$  where  $j_1 + \dots + j_n = q$ .

Then  $fg \equiv \sum a_{i_1 \dots i_n} b_{j_1 \dots j_n} x_1^{i_1+j_1} \dots x_n^{i_n+j_n}$ , where  $(i_1 + j_1) + \dots + (i_n + j_n) = p + q$ . Combining like terms, we have  $fg \equiv \sum c_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$ , where  $k_1 + \dots + k_n = p + q$ . Thus,  $fg$  is of degree  $p + q$ , unless all the coefficients are zero.

But if all the coefficients are zero, then  $fg \equiv 0$ . By the previous theorem, this is impossible. Thus, the theorem is established for homogeneous polynomials.

To consider the general case, let  $f \equiv f_0 + f_1$ , where  $f_0$  is the sum of all the terms in  $f$  of degree  $p$  with non-zero coefficients. Then  $f_0$  is homogeneous of degree  $p$  and  $f_1$  is identically zero or of degree less than  $p$ .

Similarly,  $g = g_0 + g_1$ , where  $g_0$  is homogeneous of degree  $q$  and  $g_1$  is zero or of degree less than  $q$ . Then

$$fg = f_0g_0 + f_0g_1 + f_1g_0 + f_1g_1$$

From the already established result for homogeneous polynomials,  $f_0g_0$  is of degree  $p + q$ . Also, each of  $f_0g_1, f_1g_0, f_1g_1$  is zero or of degree less than  $p + q$ . Hence,  $f_0g_1 + f_1g_0 + f_1g_1$  is zero or of degree less than  $p + q$ . Therefore,  $fg$  is of degree  $p + q$ , and the theorem is proved.

*Example* A non-constant polynomial  $f(x_1, \dots, x_n)$  is said to be irreducible (over the field of complex numbers) if it cannot be expressed as the product of two polynomials (not necessarily distinct) in  $x_1, \dots, x_n$  neither of which is a constant. Otherwise it is called reducible. Show that  $f(x, y) \equiv x^5 - 3xy + 1$  is irreducible.

Suppose  $f$  reducible and that  $f \equiv g(x, y)h(x, y)$ , where neither  $g$  nor  $h$  is a constant.

Since  $f$  is of degree 1 in  $y$ , one of  $g$  and  $h$  is of degree 1 in  $y$  and the other is of degree zero in  $y$  (see ex. 1 below). Hence  $f \equiv a(x)[b(x)y + c(x)]$ , where  $a, b, c$  are polynomials in  $x$  and  $a$  is not a constant.

Equating the coefficients of  $y$ , we have  $-3x \equiv ab$ . Since  $a$  is not a constant, this requires that  $a \equiv \alpha x$  where  $\alpha$  is a constant. Thus  $f \equiv \alpha x[b(x)y + c(x)]$ . Letting  $x = 0$ , this gives us  $1 = 0$ . This contradiction shows that  $f$  is not reducible.

### Exercises

- 1 Prove: If  $f(x_1, \dots, x_n)$  and  $g(x_1, \dots, x_n)$  are of degrees  $k$  and  $l$  respectively in  $x_n$ , then  $fg$  is of degree  $k + l$  in  $x_n$ .
- 2 If  $f^2(x_1, \dots, x_n) \equiv g^2(x_1, \dots, x_n)$ , show that either  $f \equiv g$  or  $f \equiv -g$ .
- 3 Prove: A polynomial of odd degree is not the square of a polynomial.
- 4 If  $f, g, p, q$  are polynomials in  $x_1, \dots, x_n$  such that  $f \equiv pg$  and  $g \equiv qf$ , then  $f \equiv cg$  where  $c$  is a constant.
- 5 If  $g, Q_1, Q_2, R_1, R_2$  are polynomials in  $x_1, \dots, x_n$ ,  $g$  of degree  $m$ , and each of  $R_1$  and  $R_2$  is either zero or of degree less than  $m$ , and if  $Q_1g + R_1 \equiv Q_2g + R_2$ , then  $Q_1 \equiv Q_2$  and  $R_1 \equiv R_2$ .
- 6 Let  $f \equiv f_1(x_1, \dots, x_n)f_2(x_1, \dots, x_n) \cdots f_p(x_1, \dots, x_n) \neq 0$ . Prove:
  - a) If every  $f_i$  is homogeneous, then  $f$  is homogeneous.
  - b) If  $f$  is homogeneous, then every  $f_i$  is homogeneous.

- 7** Prove: If  $f(x_1, \dots, x_n)$  is homogeneous and vanishes for all values of  $x_1, \dots, x_{n-1}$  when  $x_n = 1$ , then  $f \equiv 0$ .
- 8** Prove:  $f(x_1, x_2, \dots, x_n)$  is homogeneous of degree  $m$  if and only if  $f(yx_1, yx_2, \dots, yx_n) = y^m f(x_1, x_2, \dots, x_n)$  for all values of  $x_1, x_2, \dots, x_n, y$ .
- 9** Show that the following are irreducible:
- $xy - x + y + 1$
  - $x^2 - y^2 + 1$
  - $x^2 - xy + y^2$
  - $x + g(y)$
  - $x^2 + axy + ay^2 + 1$ , where  $a$  is a constant different from 0 and 4
- 10** Prove: If  $f(x_1, \dots, x_n)$  is not a constant then it is either irreducible or the product of irreducible polynomials.
- \*11** Let  $g_i(x_1, \dots, x_n)$  ( $i = 1, 2, \dots, k$ ) be distinct polynomials in  $x_1, \dots, x_n$ . Let  $f(x, x_1, \dots, x_n)$  be a polynomial in  $x, x_1, \dots, x_n$  such that  $f(g_i, x_1, \dots, x_n) \equiv 0$  for  $i = 1, 2, \dots, k$ . Prove:
- $$f(x, x_1, \dots, x_n) = (x - g_1)(x - g_2) \cdots (x - g_k)g(x, x_1, \dots, x_n)$$
- \*12** Prove: If  $y - r$  is a factor of  $[a_0(y)x^n + \cdots + a_n(y)][b_0(y)x^m + \cdots + b_n(y)]$ , then  $y - r$  is a factor of every  $a_i(y)$  or a factor of every  $b_i(y)$ .

**4. Elementary symmetric polynomials** Let  $f(x_1, x_2, \dots, x_n)$  be a polynomial in  $x_1, x_2, \dots, x_n$ . Let  $i_1, i_2, \dots, i_n$  be the numbers  $1, 2, \dots, n$  in any order. It may or may not happen that  $f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = f(x_1, x_2, \dots, x_n)$ . For example,

- (a) If  $f(x, y, z) \equiv x - y + z$ , then  $f(x, z, y) \equiv x - z + y \neq f(x, y, z)$ , but  $f(z, y, x) \equiv z - y + x \equiv f(x, y, z)$
- (b) If  $f(x, y, z) \equiv x^2 + y^2 + z^2$ , then  $f(x, y, z) \equiv f(x, z, y) \equiv f(y, x, z) \equiv f(y, z, x) \equiv f(z, x, y) \equiv f(z, y, x)$ .

A polynomial like the one in (b) is called a symmetric polynomial. That is,  $f(x_1, x_2, \dots, x_n)$  is said to be symmetric in  $x_1, x_2, \dots, x_n$  if  $f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) \equiv f(x_1, x_2, \dots, x_n)$  whenever  $i_1, i_2, \dots, i_n$  is any arrangement whatsoever of the numbers  $1, 2, \dots, n$ .

There are certain symmetric polynomials which are especially significant, as we shall see. These are

$$S_1(x_1, \dots, x_n) \equiv x_1 + x_2 + \cdots + x_n$$

$$S_2(x_1, \dots, x_n) \equiv x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n$$



$$S_3(x_1, \dots, x_n) \equiv x_1x_2x_3 + \dots + x_{n-2}x_{n-1}x_n$$

$$S_i(x_1, \dots, x_n) \equiv x_1 x_2 \dots x_n + \dots$$

$$S_n(x_1, \dots, x_n) \equiv x_1 x_2 \dots x_n$$

For  $i = 1, 2, \dots, n$ ,  $S_i(x_1, \dots, x_n)$  is the sum of all the products which can be formed by multiplying any  $i$  of the variables  $x_1, x_2, \dots, x_n$ . Or, to say it differently,  $S_i$  is the sum of the products of  $x_1, x_2, \dots, x_n$  taken  $i$  at a time.

It is obvious that  $S_i$  is symmetric in  $x_1, x_2, \dots, x_n$ . For, if  $j_1, j_2, \dots, j_n$  are the numbers  $1, 2, \dots, n$  in some order, the sum of all the products of  $x_{j_1}, x_{j_2}, \dots, x_{j_n}$  taken  $i$  at a time is the same as the sum of the products of  $x_1, x_2, \dots, x_n$  taken  $i$  at a time.

The  $S_i$  are called the elementary symmetric polynomials in  $x_1, x_2, \dots, x_n$ . One of the reasons for their importance is the fact that if  $x_1, x_2, \dots, x_n$  are the roots of  $x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  then  $S_i(x_1, \dots, x_n) = (-1)^i a_i$  ( $i = 1, 2, \dots, n$ ) (§4, Ch. 3).

## 5. Some properties of symmetric polynomials

### THEOREM

*If  $f$  and  $g$  are symmetric in  $x_1, \dots, x_n$ , then  $f + g$  and  $fg$  are symmetric in  $x_1, \dots, x_n$ .*

*Proof:* Let  $i_1, i_2, \dots, i_n$  be any arrangement of  $1, 2, \dots, n$ . By hypothesis,

$$f(x_1, x_2, \dots, x_n) \equiv f(x_1, x_2, \dots, x_n)$$

$$g(x_1, x_2, \dots, x_n) \equiv g(x_1, x_2, \dots, x_n)$$

Therefore

$$f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) + g(x_{i_1}, x_{i_2}, \dots, x_{i_n}) \\ = f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n)$$

Thus,  $f + g$  is symmetric. Similarly,  $fg$  is symmetric.

### COROLLARY

If  $f$  is symmetric in  $x_1, \dots, x_n$  and  $a$  is a constant, then  $af$  is symmetric in  $x_1, \dots, x_n$ .

**Proof:** This follows from the theorem by letting  $q \equiv a$ .

## COROLLARY

If  $f_i$  ( $i = 1, 2, \dots, p$ ) are symmetric in  $x_1, \dots, x_n$ , then their sum and product are symmetric in  $x_1, \dots, x_n$ .

*Proof:* This follows from the theorem by mathematical induction.

## THEOREM

If  $g_i$  ( $i = 1, 2, \dots, p$ ) are symmetric polynomials in  $x_1, \dots, x_n$  and  $f(y_1, y_2, \dots, y_p)$  is a polynomial in  $y_1, y_2, \dots, y_p$ , then  $F(x_1, x_2, \dots, x_n) \equiv f(g_1, g_2, \dots, g_p)$  is symmetric in  $x_1, x_2, \dots, x_n$ .

*Proof:* Let  $f(y_1, y_2, \dots, y_p) \equiv \sum_{i_1 + i_2 + \dots + i_p = 0}^m a_{i_1 i_2 \dots i_p} y_1^{i_1} y_2^{i_2} \dots y_p^{i_p}$

Then  $F(x_1, x_2, \dots, x_n) \equiv \sum_{i_1 + i_2 + \dots + i_p = 0}^m a_{i_1 i_2 \dots i_p} g_1^{i_1} g_2^{i_2} \dots g_p^{i_p}$

From the preceding corollaries, each of the products  $a_{i_1 i_2 \dots i_p} g_1^{i_1} g_2^{i_2} \dots g_p^{i_p}$  is symmetric in  $x_1, x_2, \dots, x_n$ . Hence, their sum is symmetric in  $x_1, x_2, \dots, x_n$ , and the theorem is proved.

## THEOREM

Let  $f_i(x_1, \dots, x_{n-1})$  ( $i = 0, 1, \dots, p$ ) be polynomials in  $x_1, \dots, x_{n-1}$  and  $f(x_1, \dots, x_{n-1}, x_n) \equiv f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n + \dots + f_p(x_1, \dots, x_{n-1})x_n^p$ . If  $f$  is symmetric in  $x_1, \dots, x_{n-1}, x_n$ , then each of the  $f_i$  is symmetric in  $x_1, \dots, x_{n-1}$ .

*Proof:* Let  $i_1, \dots, i_{n-1}$  be any arrangement of  $1, \dots, n-1$ . Then  $i_1, \dots, i_{n-1}, n$  is an arrangement of  $1, \dots, n$ . Since  $f$  is symmetric in  $x_1, \dots, x_n$ ,  $f(x_{i_1}, \dots, x_{i_{n-1}}, x_n) \equiv f(x_1, \dots, x_{n-1}, x_n)$ . Hence,

$$\begin{aligned} f_0(x_{i_1}, \dots, x_{i_{n-1}}) + f_1(x_{i_1}, \dots, x_{i_{n-1}})x_n + \dots \\ + f_p(x_{i_1}, \dots, x_{i_{n-1}})x_n^p \equiv f_0(x_1, \dots, x_{n-1}) \\ + f_1(x_1, \dots, x_{n-1})x_n + \dots + f_p(x_1, \dots, x_{n-1})x_n^p \end{aligned}$$

Therefore (ex. 1, §2),  $f_i(x_{i_1}, \dots, x_{i_{n-1}}) \equiv f_i(x_1, \dots, x_{n-1})$  for  $i = 0, 1, \dots, p$ , which proves the theorem.

## Exercises

- 1 Prove:  $f(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$  and of degree one if and only if  $f \equiv aS_1(x_1, \dots, x_n) + b$  where  $a$  and  $b$  are constants and  $a \neq 0$ .
- 2 Prove: Every polynomial in  $x$  is symmetric in  $x$ .
- 3 a) If  $f(x, y) + g(z)$  is symmetric in  $x, y, z$ , then  $f(x, y) \equiv g(x) + g(y) + c$ , where  $c$  is a constant.  
b) If  $g(z) \neq 0$  and  $f(x, y)g(z)$  is symmetric in  $x, y, z$ , then  $f(x, y) \equiv c(g(x)g(y))$ , where  $c$  is a constant.
- 4 Prove: If  $f(x, y, z)$  is a polynomial in  $x, y, z$ , then there exists a polynomial  $g(x, y, z) \neq 0$  such that  $fg$  is symmetric in  $x, y, z$ .
- 5 Let  $f = f_1(x_1, \dots, x_n) + \dots + f_p(x_1, \dots, x_n)$  where each of the  $f_i$  is a non-zero homogeneous polynomial, no two of the same degree. Prove:  $f$  is symmetric in  $x_1, \dots, x_n$  if and only if each of the  $f_i$  is symmetric in  $x_1, \dots, x_n$ .
- 6 Prove: If a symmetric polynomial in  $x_1, \dots, x_n$  is of degree  $p$  in one of the variables, it is of degree  $p$  in each variable.
- 7 Let  $S(x_1, \dots, x_i)$  ( $i = 1, 2, \dots, n$ ) be the elementary symmetric polynomials in  $x_1, \dots, x_n$  and  $t_i(x_1, \dots, x_{i-1})$  ( $i = 1, 2, \dots, n-1$ ) the elementary symmetric polynomials in  $x_1, \dots, x_{i-1}$ . Prove:
 

a) $S_1 \equiv t_1 + x_n$	*b) $t_1 \equiv S_1 - x_n$
$S_2 \equiv t_2 + x_n t_1$	$t_2 \equiv S_2 - x_n S_1 + x_n^2$
$\vdots$	$t_3 \equiv S_3 - x_n S_2 + x_n^2 S_1 - x_n^3$
$S_i \equiv t_i + x_n t_{i-1}$	$\vdots$
$\vdots$	$t_{i-1} \equiv S_{i-1} - x_n S_{i-2} + x_n^2 S_{i-3} - \dots$
$S_{n-1} \equiv t_{n-1} + x_n t_{n-2}$	$+ (-1)^n x_n^{n-2} S_1 + (-1)^{n-1} x_n^{n-1}$
$S_n \equiv x_n t_{n-1}$	
- 8 Let  $f(x_1, \dots, x_{n-1}, x_n)$  be symmetric in  $x_1, \dots, x_{n-1}$ . That is,  $f(x_1, \dots, x_{i_{n-1}}, x_n) = f(x_1, \dots, x_{i-1}, x_n)$  whenever  $i_1, \dots, i_{n-1}$  are the numbers  $1, \dots, n-1$  in any order. Prove: If  $f \equiv f_n(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n + \dots + f_p(x_1, \dots, x_{n-1})x_n^p$ , then each of the  $f_i$  is symmetric in  $x_1, \dots, x_{n-1}$ .
- 9 Prove: If  $f, g, h$  are polynomials in  $x_1, \dots, x_n$  such that  $f \equiv gh \neq 0$  and two of them are symmetric in  $x_1, \dots, x_n$ , then the third is also.
- 10 Prove: The elementary symmetric polynomials  $S_i(x_1, \dots, x_n)$  ( $i = 1, \dots, n-1$ ) are irreducible.
- 11 Prove: If  $f \equiv x_n g(x_1, \dots, x_n) \neq 0$  is symmetric in  $x_1, \dots, x_n$ , then  $f \equiv x_1 x_2 \dots x_n h(x_1, \dots, x_n)$  where  $h$  is symmetric in  $x_1, \dots, x_n$ .
- 12 If  $F = f(x_n)g(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$ , then  $F \equiv f(x_1) \dots f(x_n)h(x_1, \dots, x_n)$ , where  $h$  is symmetric in  $x_1, \dots, x_n$ . (Exercise 11 is a special case.)

**6. Fundamental theorem on symmetric polynomials** We have seen (§5) that if  $g(y_1, y_2, \dots, y_n)$  is a polynomial in  $y_1, y_2, \dots, y_n$ , then  $f(x_1, x_2, \dots, x_n) \equiv g(S_1, S_2, \dots, S_n)$  is symmetric in  $x_1, x_2, \dots, x_n$ . One of the reasons for the importance of the elementary symmetric polynomials is the fact that every symmetric polynomial in  $x_1, \dots, x_n$  is obtainable from them in this way. That is:

### THEOREM

*If  $f(x_1, x_2, \dots, x_n)$  is symmetric in  $x_1, x_2, \dots, x_n$ , then there exists a polynomial  $g(y_1, y_2, \dots, y_n)$  such that  $f(x_1, x_2, \dots, x_n) \equiv g(S_1, S_2, \dots, S_n)$ .*

*Proof:* If  $f \equiv 0$  we may take  $g \equiv 0$ . Hence, suppose  $f \neq 0$ .

If  $n = 1$  there is only one symmetric polynomial,  $S_1 \equiv x_1$ . Then  $f(x_1) \equiv f(S_1)$ . Proceeding by mathematical induction, suppose the desired result established for symmetric polynomials in  $n - 1$  variables,  $n - 1 \geq 1$ .

Write  $f(x_1, x_2, \dots, x_n)$  in the form

$$f \equiv f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n \\ + \dots + f_s(x_1, \dots, x_{n-1})x_n^s$$

Each of the  $f_i(x_1, \dots, x_{n-1})$  is symmetric in  $x_1, \dots, x_{n-1}$  (§5). Therefore, by the hypothesis of the induction,

$$f_i(x_1, \dots, x_{n-1}) \equiv g_i(t_1, \dots, t_{n-1}) \quad (i = 0, 1, \dots, s)$$

where the  $t_i$  are the elementary symmetric polynomials in  $x_1, \dots, x_{n-1}$ .

$$\text{If } g_0(y_1, y_2, \dots, y_{n-1}) \equiv \sum_{i_1+i_2+\dots+i_{n-1}=m} b_{i_1 i_2 \dots i_{n-1}} y_1^{i_1} y_2^{i_2} \dots y_{n-1}^{i_{n-1}}$$

then (ex. 7, §5)

$$\begin{aligned} g_0(t_1, t_2, \dots, t_{n-1}) &\equiv g_0(S_1 - x_n, S_2 - x_n S_1 \\ &\quad + x_n^2, \dots, S_{n-1} - x_n S_{n-2} + x_n^2 S_{n-3} \\ &\quad - \dots + (-1)^{n-1} x_n^{n-1}) \\ &\equiv \sum_{i_1+i_2+\dots+i_{n-1}=0}^m b_{i_1 i_2 \dots i_{n-1}} (S_1 - x_n)^{i_1} \\ &\quad (S_2 - x_n S_1 + x_n^2)^{i_2} \dots \\ &\quad (S_{n-1} - x_n S_{n-2} + \dots + (-1)^{n-1} x_n^{n-1})^{i_{n-1}} \end{aligned}$$

$$\begin{aligned}
 &= \sum_{j_1+j_2+\dots+j_n=0}^q c_{j_1 j_2 \dots j_n} S_1^{j_1} S_2^{j_2} \dots S_{n-1}^{j_{n-1}} x_n^{j_n} \\
 &= h_0(S_1, \dots, S_{n-1}) + h_1(S_1, \dots, S_{n-1})x_n \\
 &\quad + \dots + h_q(S_1, \dots, S_{n-1})x_n^q
 \end{aligned}$$

where the  $h_i(S_1, \dots, S_{n-1})$  are polynomials in  $S_1, \dots, S_{n-1}$ .

We may proceed in a similar way with each of the  $g_i(t_1, t_2, \dots, t_{n-1})$ . If we do and if we then substitute the results into the expression for  $f$  above, we obtain

$$f = q_0(S_1, \dots, S_{n-1}) + q_1(S_1, \dots, S_{n-1})x_n + \dots + q_u(S_1, \dots, S_{n-1})x_n^u$$

where each of the  $q_i(S_1, \dots, S_{n-1})$  is a polynomial in  $S_1, \dots, S_{n-1}$ .

The  $q_i(S_1, \dots, S_{n-1})$  may also be considered as polynomials in  $S_1, \dots, S_n$  (in which all terms involving  $S_n$  have zero coefficients). Hence, the preceding may be considered an expression for  $f$  in the form

$$(1) \quad f = P_0(S_1, \dots, S_n) + P_1(S_1, \dots, S_n)x_n + \dots + P_u(S_1, \dots, S_n)x_n^u$$

where the  $P_i(S_1, \dots, S_n)$  are polynomials in  $S_1, \dots, S_n$ .

We now show that if  $u \geq n$  we can replace the right side of (1) by another expression of the same form in which  $u \leq n-1$ .

Let

$$\begin{aligned}
 g(x, x_1, \dots, x_n) &\equiv (x - x_1)(x - x_2) \dots (x - x_n) \\
 &\equiv x^n - S_1 x^{n-1} + S_2 x^{n-2} - \dots + (-1)^n S_n
 \end{aligned}$$

Since  $g(x_n, x_1, \dots, x_n) = 0$ ,

$$x_n^n \equiv S_1 x_n^{n-1} - S_2 x_n^{n-2} + \dots - (-1)^n S_n$$

Multiplying both sides by  $x_n$ , we have

$$\begin{aligned}
 x_n^{n+1} &\equiv S_1 x_n^n - S_2 x_n^{n-1} + \dots - (-1)^n S_n x_n \\
 &\equiv S_1 [S_1 x_n^{n-1} - S_2 x_n^{n-2} + \dots - (-1)^n S_n] - S_2 x_n^{n-1} \\
 &\quad + \dots - (-1)^n S_n x_n \\
 &\equiv T_1 x_n^{n-1} + T_2 x_n^{n-2} + \dots + T_n
 \end{aligned}$$

where the  $T_i$  are polynomials in  $S_1, \dots, S_n$ .

If we multiply both sides of the last equality by  $x_n$  and proceed in a similar way, we find a similar expression for  $x_n^{n+2}$ .

If  $u \geq n$  we can continue in this way until we have  $x_n^n, x_n^{n+1}, \dots, x_n^u$  all expressed in this form. If we then make these replacements in the right side of (1), we obtain an expression for  $f$  in the form (1) in which  $u \leq n-1$ .

Suppose, therefore, that  $u \leq n-1$  in (1). We now show that  $P_1(S_1, \dots, S_n) = P_2(S_1, \dots, S_n) = \dots = P_u(S_1, \dots, S_n) = 0$  for all values of  $x_1, \dots, x_n$ .

If  $u = 0$  there is, of course, nothing to be proved. Suppose  $u > 0$ .

Let

$$h(x, x_1, \dots, x_n) \equiv [P_0(S_1, \dots, S_n) - f(x_1, \dots, x_n)] \\ + P_1(S_1, \dots, S_n)x + \dots + P_u(S_1, \dots, S_n)x^u$$

Since  $f(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$ , interchanging  $x_n$  and  $x_k$  leaves  $f(x_1, \dots, x_n)$  unchanged. It also leaves each of the  $P_i(S_1, \dots, S_n)$  unchanged (§5). Therefore, interchanging  $x_n$  and  $x_k$  in (1), we have

$$f(x_1, \dots, x_n) \equiv P_0(S_1, \dots, S_n) + P_1(S_1, \dots, S_n)x_k \\ + \dots + P_u(S_1, \dots, S_n)x_k^u$$

for all values of  $x_1, \dots, x_n$ . Thus,

$$h(x_1, x_1, \dots, x_n) = 0 \quad \text{for } l = 1, 2, \dots, n$$

By ex. 11, §3, either  $h(x_1, x_1, \dots, x_n) = 0$  or else its degree in  $x$  is at least  $n$ . Since  $u < n$ , the latter is impossible. Therefore,  $h(x_1, x_1, \dots, x_n) = 0$ . Hence, for  $l = 1, 2, \dots, u$ ,  $P_l(S_1, \dots, S_n) = 0$  for all values of  $x_1, \dots, x_n$ .

Therefore,  $f = P_0(S_1, \dots, S_n)$  for all values of  $x_1, \dots, x_n$ , which establishes the desired result.

Thus, the theorem is proved.

*Example* Express  $x_1^3 + x_2^3 + x_3^3$  in terms of the elementary symmetric polynomials.

We shall proceed by the method used in the proof of the theorem. We have

$$S_1 \equiv x_1 + x_2 + x_3 \equiv t_1 + x_3 \quad \text{where } t_1 \equiv x_1 + x_2$$

$$S_2 \equiv x_1x_2 + x_1x_3 + x_2x_3 \equiv t_2 + t_1x_3 \quad \text{where } t_2 \equiv x_1x_2$$

$$S_3 \equiv x_1x_2x_3 \equiv t_3x_3$$

$$\begin{aligned} f(x_1, x_2, x_3) &\equiv (x_1^3 + x_2^3) + x_3^3 \\ &\equiv (t_1^3 - 3t_1t_2) + x_3^3 \\ &\equiv (S_1 - x_3)^3 - 3(S_1 - x_3)(S_2 - S_1x_3 + x_3^2) + x_3^3 \\ &\equiv (S_1^3 - 3S_1S_2) + 3S_2x_3 - 3S_1x_3^2 + 3x_3^3 \end{aligned}$$

$$\begin{aligned}
g(x, x_1, x_2, x_3) &\equiv (x - x_1)(x - x_2)(x - x_3) \\
&\equiv x^3 - S_1x^2 + S_2x - S_3 \\
x_3^2 &\equiv S_1x_3^2 - S_2x_3 + S_3 \\
f(x_1, x_2, x_3) &\equiv S_1^3 - 3S_1S_2 + 3S_2x_3 - 3S_1x_3^2 \\
&\quad + 3(S_1x_3^2 - S_2x_3 + S_3) \\
&\equiv S_1^3 - 3S_1S_2 + 3S_3
\end{aligned}$$

In general, if  $f(x_1, \dots, x_n)$  is symmetric it may not be so easy to obtain  $g(y_1, \dots, y_n)$  so that  $g(S_1, \dots, S_n) = f(x_1, \dots, x_n)$ . The discussion in the following paragraph will often be found helpful.

### Exercises

- 1 a) If  $a_1, \dots, a_n$  are any complex numbers, show that there are values of  $x_1, \dots, x_n$  such that  $S_i(x_1, \dots, x_n) = a_i$  for  $i = 1, 2, \dots, n$ . [Hint: Consider the roots of  $x^n - a_1x^{n-1} + \dots + (-1)^na_n$ .]
- \*b) Prove: If  $g(y_1, \dots, y_n)$  is a polynomial such that  $g(S_1, \dots, S_n)$  vanishes for all values of  $x_1, \dots, x_n$ , then  $g(y_1, \dots, y_n) \equiv 0$ . [Hint: Use (a).]
- c) If  $f(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$ , show that there is only one polynomial  $g(y_1, \dots, y_n)$  such that  $f \equiv g(S_1, \dots, S_n)$ . [Hint: Use (b).]
- 2 By following through all the steps in the proof of the theorem above, show (by mathematical induction) that if  $a_1, a_2, \dots, a_n$  are the coefficients in  $f(x_1, \dots, x_n)$ , in any order, then every coefficient in  $g(y_1, \dots, y_n)$  has the form  $c_1 + c_2a_2 + \dots + c_na_n$ , where the  $c$ 's are integers (positive, negative, or zero).
- 3 Let  $f_i \equiv a_iS_1 + g_i(S_1, \dots, S_{i-1})$  ( $i = 1, \dots, n$ ), where  $a_i \neq 0$  is a constant and  $g_i$  is a polynomial in  $S_1, \dots, S_{i-1}$ . Show that every polynomial symmetric in  $x_1, \dots, x_n$  is a polynomial in  $f_1, \dots, f_n$ . Show also that this polynomial is unique.
- 4 Prove: If  $f(x_1, \dots, x_{n-1}, x_n)$  is symmetric in  $x_1, \dots, x_{n-1}$ , there exists a polynomial  $g(y_1, \dots, y_{n-1}, y_n)$  such that  $f \equiv g(t_1, \dots, t_{n-1}, x_n)$ , where  $t_1, \dots, t_{n-1}$  are the elementary symmetric polynomials in  $x_1, \dots, x_{n-1}$ .

## 7. Weight

### THEOREM

If  $f(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$  and is homogeneous of degree  $m$ , and if  $f \equiv g(S_1, \dots, S_n)$  where  $g(y_1, \dots, y_n) \equiv \sum b_{i_1 \dots i_n} y_1^{i_1} \dots y_n^{i_n}$ , then  $b_{i_1 \dots i_n} = 0$  if  $i_1 + 2i_2 + \dots + ni_n \neq m$ .

If  $b_1 \dots b_n \neq 0$ ,  $i_1 + 2i_2 + \dots + ni_n$  is called the weight of the term  $b_1 \dots b_n y_1^{i_1} \dots y_n^{i_n}$ .

*Proof:* Group the terms of  $g(y_1, \dots, y_n)$  according to their weights, putting into one group all terms having a common weight. Then

$$g(y_1, \dots, y_n) \equiv g_1(y_1, \dots, y_n) + \dots + g_p(y_1, \dots, y_n) \\ (p \geq 1)$$

where in each  $g_i(y_1, \dots, y_n)$  all the terms have the same weight  $\mu_i$ , and the  $\mu_i$ 's (if  $p > 1$ ) are distinct. Then

$$f(x_1, \dots, x_n) \equiv g_1(S_1, \dots, S_n) + \dots + g_p(S_1, \dots, S_n) \\ \equiv f_1(x_1, \dots, x_n) + \dots + f_p(x_1, \dots, x_n)$$

where  $f_i(x_1, \dots, x_n) \equiv g_i(S_1, \dots, S_n)$ .

Since  $S_1$  is homogeneous in  $x_1, \dots, x_n$  of degree 1,  $S_2$  homogeneous of degree 2, etc,  $S_1^{i_1} \dots S_n^{i_n}$  is homogeneous in  $x_1, \dots, x_n$  of degree  $i_1 + 2i_2 + \dots + ni_n$ . Hence all the terms in  $f_i(x_1, \dots, x_n) = g_i(S_1, \dots, S_n)$  are of the same degree  $\mu_i$  in  $x_1, \dots, x_n$ . Therefore,  $f_i(x_1, \dots, x_n)$  is homogeneous in  $x_1, \dots, x_n$  of degree  $\mu_i$  or else it vanishes identically in  $x_1, \dots, x_n$ .

Since  $f$  is homogeneous in  $x_1, \dots, x_n$  of degree  $m$ , all the  $f_i$  must be identically zero in  $x_1, \dots, x_n$  except the one for which  $\mu_i = m$ .

But if  $f_i(x_1, \dots, x_n) = g_i(S_1, \dots, S_n)$  vanishes for all  $x_1, \dots, x_n$ , then  $g_i(y_1, \dots, y_n) \equiv 0$  (ex. 1(b), §6). Hence, the theorem is proved

### THEOREM

If  $f(x_1, \dots, x_n)$  is symmetric in  $x_1, \dots, x_n$  and of degree  $m$ , and if  $f \equiv g(S_1, \dots, S_n)$  where  $g(y_1, \dots, y_n) \equiv \sum b_1 \dots b_n y_1^{i_1} \dots y_n^{i_n}$ , then  $b_1 \dots b_n = 0$  if  $i_1 + 2i_2 + \dots + ni_n > m$

*Proof:* Proceeding as above, we see that all the  $g_i(y_1, \dots, y_n)$  vanish identically except possibly those for which  $\mu_i \leq m$ .

*Example* We work again the example of §6, where  $f \equiv x_1^3 + x_2^3 + x_3^3$ .

Since  $f$  is homogeneous of degree 3,  $g(y_1, y_2, y_3) \equiv \sum b_{i_1 i_2 i_3} y_1^{i_1} y_2^{i_2} y_3^{i_3}$  where  $i_1 + 2i_2 + 3i_3 = 3$ . The only possible values of  $i_1, i_2, i_3$  are 0, 0, 1 or 3, 0, 0 or 1, 1, 0. Hence  $g \equiv ay_3 + by_1^3 + cy_1y_2$



where  $a, b, c$  are constants. Thus,

$$x_1^3 + x_2^3 + x_3^3 \equiv ax_1x_2x_3 + b(x_1 + x_2 + x_3)^3 + c(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3)$$

To determine  $a, b, c$  we may equate coefficients of like terms on both sides or we may let  $x_1, x_2, x_3$  have special values, or we may use a combination of both methods.

If we let  $x_3 = 0$  we obtain

$$x_1^3 + x_2^3 \equiv b(x_1 + x_2)^3 + c(x_1 + x_2)x_1x_2$$

Equating coefficients of  $x_1^3$  we obtain  $b = 1$ . Letting  $x_1 = x_2 = 1$  in the same equation, we obtain  $8 + 2c = 2$ , so that  $c = -3$ . Thus.

$$x_1^3 + x_2^3 + x_3^3 \equiv ax_1x_2x_3 + (x_1 + x_2 + x_3)^3 - 3(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3)$$

Now letting  $x_1 = x_2 = x_3 = 1$ , we obtain  $a = 3$ , which determines the last of the constants.

### Exercises

1 Express each of the following in terms of the elementary symmetric polynomials:

- $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$
- $x_1^2x_2^2x_3^2 + x_1^2x_2^2x_4^2 + x_1^2x_3^2x_4^2 + x_2^2x_3^2x_4^2$
- $x_1x_2^2x_3x_4 + x_1x_2^2x_3x_1 + x_1x_2^2x_3x_1 + x_1^2x_2x_3x_4 + x_1^2x_2x_3x_4 + x_1^2x_2^2x_3x_4$
- $x_1x_2^2x_3^2 + x_1^2x_2x_3^2 + x_1^2x_2^2x_3$
- $(x_1 + x_2)x_3^2 + (x_1 + x_2)x_4^2 + (x_1 + x_2)x_1^2$
- $x_1^2x_2 + x_1^2x_3 + x_1^2x_4 + x_2^2x_1 + x_2^2x_3 + x_2^2x_4 + x_3^2x_1 + x_3^2x_2 + x_3^2x_4 + x_4^2x_1 + x_4^2x_2 + x_4^2x_3$
- $x_1^4 + x_2^4 + x_3^4$
- $(x_1 + x_2 + x_3)(x_1 + x_2 + x_1) + (x_1 + x_2 + x_3)(x_1 + x_3 + x_4) + (x_1 + x_2 + x_1)(x_1 + x_3 + x_1) + (x_1 + x_2 + x_1)(x_2 + x_3 + x_4) + (x_1 + x_2 + x_1)(x_2 + x_3 + x_1) + (x_1 + x_3 + x_4)(x_2 + x_3 + x_4)$
- $(x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$
- $(x_1 + x_2 - x_3)(x_1 + x_3 - x_2)(x_2 + x_3 - x_1)$
- $x_1^3 + x_2^3 + x_3^3 + x_4^3$
- $x_1(x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2) + x_2(x_1^2x_3^2 + x_1^2x_4^2 + x_3^2x_4^2) + x_3(x_1^2x_2^2 + x_1^2x_4^2 + x_2^2x_4^2) + x_4(x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2)$

2 Express  $f_0$  in terms of the other  $f$ 's (see ex. 3, §6):

- $f_0 \equiv x_1^3 + x_2^3, f_1 \equiv x_1 + x_2 + 1, f_2 \equiv x_1x_2 - x_1 - x_2$
- $f_0 \equiv x_1^3 + x_2^3, f_1 \equiv x_1 + x_2, f_2 \equiv x_1^2 + x_2^2$

- c)  $f_0 \equiv x_1x_2^2 + x_1x_3^2 + x_2x_3^2 + x_2x_1^2 + x_3x_1^2 + x_3x_2^2$ ,  $f_1 \equiv x_1 + x_2 + x_3$ ,  
 $f_2 \equiv x_1^2 + x_2^2 + x_3^2$ ,  $f_3 \equiv x_1x_2x_3$
- d)  $f_0 \equiv x_1^3 + x_2^3 + x_3^3$ ,  $f_1 \equiv S_1(x_1, x_2, x_3)$ ,  $f_2 \equiv S_1(x_1, x_2, x_3) + S_2(x_1, x_2, x_3)$ ,  
 $f_3 \equiv S_1(x_1, x_2, x_3) + S_2(x_1, x_2, x_3) + S_3(x_1, x_2, x_3)$
- e)  $f_0 \equiv x_1x_2x_3$ ,  $f_1 \equiv x_1 + x_2 + x_3 - 1$ ,  $f_2 \equiv x_1x_2 + x_1x_3 + x_2x_3$ ,  
 $f_3 \equiv x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2$
- f)  $f_0 \equiv x_1^3x_2^2 + x_1^2x_3^2 + x_1^3x_4^2 + x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2$ ,  $f_1 \equiv S_1(x_1, x_2, x_3, x_4)$ ,  
 $f_2 \equiv S_2(x_1, x_2, x_3, x_4) - S_1^2(x_1, x_2, x_3, x_4)$ ,  $f_3 \equiv S_3(x_1, x_2, x_3, x_4) -$   
 $S_2(x_1, x_2, x_3, x_4) - S_1^2(x_1, x_2, x_3, x_4)$ ,  $f_4 \equiv S_4(x_1, x_2, x_3, x_4) +$   
 $3S_3(x_1, x_2, x_3, x_4) + 2S_2(x_1, x_2, x_3, x_4) + S_1(x_1, x_2, x_3, x_4)$

## DETERMINANTS

1. Introduction If we solve the simultaneous equations

$$a_1x + b_1y = c_1$$

$$a_2x + b_2y = c_2$$

for  $x$  and  $y$ , we find

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1}, \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}$$

provided  $a_1b_2 - a_2b_1 \neq 0$ .

The expressions  $a_1b_2 - a_2b_1$ ,  $c_1b_2 - c_2b_1$ ,  $a_1c_2 - a_2c_1$  have similar forms. The second is obtainable from the first by replacing  $a_1, a_2$  by  $c_1, c_2$  respectively. The third is obtainable from the first by replacing  $b_1, b_2$  by  $c_1, c_2$  respectively. If we denote  $a_1b_2 - a_2b_1$  by  $D(a_1, a_2, b_1, b_2)$ , then

$$x = \frac{D(c_1, c_2, b_1, b_2)}{D(a_1, a_2, b_1, b_2)}, \quad y = \frac{D(a_1, a_2, c_1, c_2)}{D(a_1, a_2, b_1, b_2)}$$

If we have three simultaneous equations

$$a_1x + b_1y + c_1z = d_1$$

$$a_2x + b_2y + c_2z = d_2$$

$$a_3x + b_3y + c_3z = d_3$$

and if we solve for  $x, y, z$ , we obtain

$$\begin{aligned} x &= \frac{d_1b_2c_3 - d_1b_3c_2 - d_2b_1c_3 + d_2b_3c_1 + d_3b_1c_2 - d_3b_2c_1}{a_1b_2c_3 - a_1b_3c_2 - a_2b_1c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1} \\ y &= \frac{a_1d_2c_3 - a_1d_3c_2 - a_2d_1c_3 + a_2d_3c_1 + a_3d_1c_2 - a_3d_2c_1}{a_1b_2c_3 - a_1b_3c_2 - a_2b_1c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1} \\ z &= \frac{a_1b_2d_3 - a_1b_3d_2 - a_2b_1d_3 + a_2b_3d_1 + a_3b_1d_2 - a_3b_2d_1}{a_1b_2c_3 - a_1b_3c_2 - a_2b_1c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1} \end{aligned}$$

provided  $a_1b_2c_3 - a_1b_3c_2 - a_2b_1c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1 \neq 0$ .

The four expressions in the numerators and denominators have similar forms. For instance, the numerator in the expression for  $y$  is obtainable from the denominator by replacing  $b_1, b_2, b_3$  by  $d_1, d_2, d_3$  respectively.

If we denote the common denominator in the three expressions by  $D(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3)$ , then

$$\begin{aligned}x &= \frac{D(d_1, d_2, d_3, b_1, b_2, b_3, c_1, c_2, c_3)}{D(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3)} \\y &= \frac{D(a_1, a_2, a_3, d_1, d_2, d_3, c_1, c_2, c_3)}{D(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3)} \\z &= \frac{D(a_1, a_2, a_3, b_1, b_2, b_3, d_1, d_2, d_3)}{D(a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3)}\end{aligned}$$

What we have done for simultaneous equations in two or three unknowns can be carried out in general for  $n$  simultaneous linear equations in  $n$  unknowns, but the expressions involved become more and more complicated as  $n$  increases. To obtain a general rule for solving  $n$  linear equations in  $n$  unknowns in a form convenient to use and easy to remember, it is desirable to have an appropriate way of writing the complicated expressions that appear. Fortunately, the theory of determinants provides such a way.

We devote this chapter to a brief introduction to the theory of determinants which we apply in the following chapter to solving simultaneous linear equations.

**2. Definition of determinant** Consider the  $n^2$  numbers or variables  $a_{ij}$ , where  $i$  and  $j$  have integral values from 1 to  $n$  inclusive, arranged in a square array as follows:

$$(1) \quad \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ . & . & . & \cdots & . \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}$$

Such an array is called a square matrix. More fully, it is an  $n$ -rowed square matrix, or a square matrix of order  $n$ . (Later, §9, we shall consider more general matrices, i.e., rectangular arrays in which the number of rows may or may not equal the number of columns).

The  $a_{ij}$  are called the elements of the matrix. The first number,  $i$ , in the double subscript shows the number of the (horizontal) row, counting from the top, in which the element lies and the second,  $j$ , the number of the (vertical) column, counting from the left. For example, the element in the fourth row and fifth column is  $a_{45}$ .

We define what is called the determinant of the matrix (1) denoted by

$$(2) \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{vmatrix}$$

For  $n = 1$  we define  $|a_{11}| = a_{11}$

For  $n = 2$  we define

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}|a_{22}| - a_{12}|a_{21}| = a_{11}a_{22} - a_{12}a_{21}$$

For  $n = 3$  we define

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} \\ = a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) \\ + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

In general, suppose we have defined the determinant of an  $(n-1)$ -rowed square matrix. Consider the  $n$ -rowed square matrix (1). Let  $A_{ij}$  ( $i, j = 1, 2, \dots, n$ ) denote the determinant of the  $(n-1)$ -rowed square matrix obtained by deleting from (1) all the elements in the first row and all the elements in column  $j$ . We define the determinant of (1) as

$$(3) \quad a_{11}A_{11} - a_{12}A_{12} + a_{13}A_{13} - \cdots + (-1)^{n-1}a_{1n}A_{1n}.$$

By the principle of mathematical induction, this defines the determinant of every square matrix.

The elements, rows and columns of (1) are also called the elements, rows and columns of (2).

For brevity, we usually refer to (2) as a determinant, or a determinant of order  $n$ , rather than "the determinant of the matrix (1)."

**Example** Evaluate the determinant

$$D = \begin{vmatrix} 5 & 0 & 0 & 4 \\ -1 & 2 & 0 & 0 \\ 0 & 3 & -4 & 0 \\ 2 & -2 & 3 & 3 \end{vmatrix}$$

We have

$$D = 5 \begin{vmatrix} 2 & 0 & 0 \\ 3 & -4 & 0 \\ -2 & 3 & 3 \end{vmatrix} - 0 \begin{vmatrix} -1 & 0 & 0 \\ 0 & -4 & 0 \\ 2 & 3 & 3 \end{vmatrix} + 0 \begin{vmatrix} -1 & 2 & 0 \\ 0 & 3 & 0 \\ 2 & -2 & 3 \end{vmatrix} - 4 \begin{vmatrix} -1 & 2 & 0 \\ 0 & 3 & -4 \\ 2 & -2 & 3 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 0 & 0 \\ 3 & -4 & 0 \\ -2 & 3 & 3 \end{vmatrix} = 2 \begin{vmatrix} -4 & 0 \\ 3 & 3 \end{vmatrix} - 0 \begin{vmatrix} 3 & 0 \\ -2 & 3 \end{vmatrix} + 0 \begin{vmatrix} 3 & -4 \\ -2 & 3 \end{vmatrix} = 2(-12 - 0) = -24$$

$$\begin{vmatrix} -1 & 2 & 0 \\ 0 & 3 & -4 \\ 2 & -2 & 3 \end{vmatrix} = -1 \begin{vmatrix} 3 & -4 \\ -2 & 3 \end{vmatrix} - 2 \begin{vmatrix} 0 & -4 \\ 2 & 3 \end{vmatrix} + 0 \begin{vmatrix} 0 & 3 \\ 2 & -2 \end{vmatrix} = -(9 - 8) - 2(0 + 8) = -17$$

$$D = 5(-24) - 4(-17) = -52$$

**3. Expansion of a determinant** For  $n = 1, 2, 3$  it is evident that a determinant of order  $n$  is a polynomial in its elements. By mathematical induction it is easily shown that the same is true of a determinant of any order.

The expression for a determinant as a polynomial in its elements is called the expansion of the determinant, and each term in the expansion is called a term of the determinant.

The expansion of a determinant has a rather simple form, as shown by:

#### THEOREM

*The determinant (2) is the sum of all possible products  $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ , where  $j_1, j_2, \dots, j_n$  are the integers 1, 2,  $\dots$ ,  $n$  in any order, each multiplied by either 1 or  $-1$ .*

**Proof:** For  $n = 1, 2$  this is obvious. Suppose it true for determinants of order  $n - 1$ . Then, by (3), for a determinant  $D$  of



**4 Prove:** There are  $n!$  terms in the expansion of a determinant of order  $n$ .

**5 Prove:** If all the elements in one row, or all the elements in one column, of a determinant are zero, then the determinant is zero.

**6 Prove:** If all but  $n - 1$  elements in a determinant of order  $n$  are zero, then the determinant is zero.

**7 Prove:**

$$\begin{vmatrix} a_{11} & 0 & 0 & \cdots & 0 & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 & 0 \\ a_{31} & a_{32} & a_{33} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \cdots & a_{n-1,n-1} & 0 \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{n,n-1} & a_{nn} \end{vmatrix} = a_{11}a_{22}a_{33} \cdots a_{nn}$$

[In a determinant of order  $n$  the elements  $a_{ii}$  ( $i = 1, 2, \dots, n$ ) are called the elements of the main diagonal.]

**\*8 Prove:** If all the elements of one row, or all the elements of one column, are multiplied by  $\lambda$ , then the determinant is multiplied by  $\lambda$ .

**\*9 Prove:**

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,n} \\ a_{i,1} + b_{i,1} & a_{i,2} + b_{i,2} & \cdots & a_{i,n} + b_{i,n} \\ a_{i+1,1} & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,n} \\ a_{i,1} & a_{i,2} & \cdots & a_{i,n} \\ a_{i+1,1} & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,n} \\ b_{i,1} & b_{i,2} & \cdots & b_{i,n} \\ a_{i+1,1} & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

**10 Prove:** If every element of a determinant is a polynomial in  $x$ , then the determinant is a polynomial in  $x$ .

**11** If  $j_1, j_2, \dots, j_n$  is an arrangement of  $n$  distinct positive integers, the number of inversions in the arrangement is defined as the number of times a larger integer precedes a smaller one. For example, in 7, 2, 1, 4 there are four inversions (7 before 2, 7 before 1, 7 before 4, 2 before 1). If  $j_1, j_2, \dots, j_n$  are the integers 1, 2,  $\dots, n$  in some order and  $N$  is the number of inversions, prove  $N = (j_1 - 1) + (\text{the number of inversions in } j_2, \dots, j_n)$ . Show then that the sign of the term  $\pm a_{1j_1} \cdots a_{nj_n}$  in the expansion of the determinant  $D$  is the sign of  $(-1)^N$ .



**4. Cofactors** In the definition of a determinant the elements of the first row play a special role. This distinction, however, is only an apparent one; we now show that a determinant can be expressed in a similar way using the elements of any row.

If  $a_{ij}$  is an element of the determinant  $D$  of order  $n$ , the determinant of order  $n - 1$  obtained by deleting from  $D$  all the elements in row  $i$  and all the elements in column  $j$  is called the complement of  $a_{ij}$ ; we shall denote it by  $A_{ij}$ .

### THEOREM

For any  $i$  between 1 and  $n$  inclusive

$$D = (-1)^{i+1}[a_{i1}A_{i1} - a_{i2}A_{i2} + a_{i3}A_{i3} - \cdots + (-1)^{n-1}a_{in}A_{in}]$$

For  $i = 1$  this is exactly the definition (3).

*Proof:* For  $n = 1$  there is nothing to be proved. For  $n = 2$  it is easily verified.

Proceeding by mathematical induction, suppose it true for determinants of order  $n - 1 \geq 2$ . Consider the determinant of order  $n$  given by (2).

For  $i = 1$  there is nothing to be proved. Hence, suppose  $i > 1$ .

Let  $C_{\alpha\beta}$  denote the determinant of order  $n - 2$  obtained from  $D$  by deleting the elements in the first row and also those in row  $i$ , as well as all the elements in columns  $\alpha$  and  $\beta$ .

Applying the hypothesis of the induction to each of the determinants  $A_{11}$ ,  $A_{12}$ ,  $\cdots$ ,  $A_{1n}$  appearing in (3) (noting that for each of these determinants the row containing  $a_{i1}$ ,  $a_{i2}$ ,  $\cdots$ ,  $a_{in}$  is row number  $i - 1$ ), we have

$$\begin{aligned} A_{11} &= (-1)^1[a_{i2}C_{12} - a_{i3}C_{13} + a_{i4}C_{14} - \cdots + (-1)^{n-2}a_{in}C_{1n}] \\ A_{12} &= (-1)^1[a_{i1}C_{21} - a_{i3}C_{23} + a_{i4}C_{24} - \cdots + (-1)^{n-2}a_{in}C_{2n}] \\ A_{13} &= (-1)^1[a_{i1}C_{31} - a_{i2}C_{32} + a_{i4}C_{34} - \cdots + (-1)^{n-2}a_{in}C_{3n}] \\ &\vdots \\ A_{1n} &= (-1)^1[a_{i1}C_{n1} - a_{i2}C_{n2} + a_{i3}C_{n3} - \cdots \\ &\quad + (-1)^{n-2}a_{i,n-1}C_{n,n-1}] \end{aligned}$$

Hence, by (3),

$$\begin{aligned} D &= (-1)^1a_{11}[a_{i2}C'_{12} - a_{i3}C_{13} + a_{i4}C_{14} - \cdots + (-1)^{n-2}a_{in}C_{1n}] \\ &\quad - (-1)^1a_{12}[a_{i1}C_{21} - a_{i3}C_{23} + a_{i4}C_{24} - \cdots + (-1)^{n-2}a_{in}C_{2n}] \\ &\quad + (-1)^1a_{13}[a_{i1}C_{31} - a_{i2}C_{32} + a_{i4}C_{34} - \cdots + (-1)^{n-2}a_{in}C_{3n}] \\ &\quad \vdots \\ &\quad + (-1)^{n-1}(-1)^1a_{1n}[a_{i1}C_{n1} - a_{i2}C_{n2} + a_{i3}C_{n3} - \cdots \\ &\quad \quad + (-1)^{n-2}a_{i,n-1}C_{n,n-1}] \end{aligned}$$



as compared to the columns. Again, this distinction is only an apparent one, for we now prove:

### THEOREM

*If each of the elements in any one column be multiplied by its cofactor, the sum of the products is the value of the determinant.*

*Proof:* Consider the  $j$ th column of the determinant  $D$  of order  $n$ . Then (§3) every term in the expansion of  $D$  has as a factor one and only one element of column  $j$ . Hence, grouping the terms according to which of  $a_{1j}, a_{2j}, \dots, a_{nj}$  they have as a factor, we may write

$$D = a_{1j}\varphi_1 + a_{2j}\varphi_2 + \dots + a_{nj}\varphi_n$$

$a_{ij}\varphi_i$  contains all the terms of  $D$  which have  $a_{ij}$  as a factor. But, these terms are exactly  $a_{ij}B_{ij}$ , where  $B_{ij}$  is the cofactor of  $a_{ij}$ , as we can see by expanding  $D$  according to row  $i$ . Thus,

$$D = a_{1j}B_{1j} + a_{2j}B_{2j} + \dots + a_{nj}B_{nj}$$

and the theorem is proved.

6. Interchange of rows and columns Let  $D$  be the determinant (2) and  $D'$  the determinant obtained from  $D$  by interchanging the rows and columns of  $D$ . That is,

$$D' = \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \cdot & \cdot & \dots & \cdot \\ b_{n1} & b_{n2} & \cdot & b_{nn} \end{vmatrix}$$

where  $b_{ij} = a_{ji}$  for all values of  $i$  and  $j$ .

$D'$  is called the transpose of  $D$ .

### THEOREM

*A determinant is identical with its transpose.*

*Proof:* For  $n = 1$  there is nothing to be proved and for  $n = 2$  the theorem is easily verified. Hence, proceeding by mathematical induction, suppose the desired result established for determinants of order  $n - 1 \geq 2$  and consider a determinant  $D$  of order  $n$ .

If  $A_{ij}$  is the complement of  $a_{ij}$  in  $D$ , the complement of  $a_{ij}$  in  $D'$  is the transpose of  $a_{ij}$ . By the hypothesis of the induction, the

transpose of  $A_{ij}$  is identical with  $A_{ji}$ . Hence, the cofactor of  $a_{ij}$  in  $D'$  is  $(-1)^{i+j}A_{ji}$ , which is also the cofactor of  $a_{ij}$  in  $D$ .

Thus, if we expand  $D'$  according to its first column, the result is identical with the expansion of  $D$  according to its first row. Hence,  $D'$  is identical with  $D$ , so that, by the principle of mathematical induction, the theorem is proved.

By virtue of this theorem, from a theorem concerning the rows of a determinant we can immediately deduce a corresponding result about the columns, and vice versa. For instance, in §7 we show that interchanging two rows of a determinant changes the sign of the determinant. From this we can conclude that interchanging two columns also changes the sign of a determinant. For, if  $D'$  is the transpose of  $D$ ,  $D_1$  the determinant obtained from  $D$  by interchanging columns  $i$  and  $j$ ,  $D'_1$  the determinant obtained from  $D'$  by interchanging rows  $i$  and  $j$ , then  $D = D'$  and  $D_1 = D'_1$ . But  $D'_1 = -D'$ . Hence  $D_1 = -D$ .

## 7. Some properties of determinants

### THEOREM

*If determinant  $D_1$  is obtained from determinant  $D$  by interchanging two rows (or two columns) of  $D$ , then  $D_1 = -D$ .*

*Proof:* For  $n = 2$  this is easily verified. Proceeding by mathematical induction, suppose it true for determinants of order  $n - 1 \geq 2$ .

Let rows  $i$  and  $j$  be interchanged in the determinant  $D$  of order  $n$ . Since  $n \geq 3$ , there is a row, say row number  $k$ , which is not disturbed. Expand both  $D$  and  $D_1$  according to this row. Then

$$\begin{aligned} D &= (-1)^{k+1}[a_{k1}A_{k1} - a_{k2}A_{k2} + \cdots + (-1)^{n-1}a_{kn}A_{kn}] \\ D_1 &= (-1)^{k+1}[a_{k1}B_{k1} - a_{k2}B_{k2} + \cdots + (-1)^{n-1}a_{kn}B_{kn}] \end{aligned}$$

where  $A_{k1}, A_{k2}, \dots, A_{kn}$  are the complements of  $a_{k1}, a_{k2}, \dots, a_{kn}$  in  $D$  and  $B_{k1}, B_{k2}, \dots, B_{kn}$  are the complements of  $a_{k1}, a_{k2}, \dots, a_{kn}$  in  $D_1$ .

$B_{k1}$  is obtainable from  $A_{k1}$  by interchanging the row containing  $a_{i2}, a_{i3}, \dots, a_{in}$  and the row containing  $a_{j2}, a_{j3}, \dots, a_{jn}$ . Therefore, by the hypothesis of the induction,  $B_{k1} = -A_{k1}$ .

Similarly,  $B_{k2} = -A_{k2}, \dots, B_{kn} = -A_{kn}$ .

The desired result now follows immediately, and the theorem is proved for the interchange of two rows.

The theorem for the interchange of two columns can be established in a similar way, or by using the theorem of §6.

### THEOREM

*If two rows (or columns) of a determinant are identical, the determinant is zero.*

*Proof:* If  $D_1$  is the determinant obtained by interchanging the two identical rows (or columns) of  $D$ , then  $D_1 = -D$  by the previous theorem. But, since these two rows (or columns) are identical,  $D_1 = D$ . Hence,  $D = -D$ ,  $2D = 0$ ,  $D = 0$ .

### THEOREM

*If the elements of one row (or column) of a determinant are changed by adding to them a common multiple of the corresponding elements of another row (or column), the value of the determinant is unchanged.*

More precisely, if  $i$  and  $j$  are distinct integers between 1 and  $n$  inclusive, then (stating the theorem for rows)

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & a_{i-1,2} & \cdots & a_{i-1,n} \\ a_{i,1} + \lambda a_{j,1} & a_{i,2} + \lambda a_{j,2} & \cdots & a_{i,n} + \lambda a_{j,n} \\ a_{i+1,1} & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j-1,1} & a_{j-1,2} & \cdots & a_{j-1,n} \\ a_{j,1} & a_{j,2} & \cdots & a_{j,n} \\ a_{i+1,1} & a_{i+1,2} & \cdots & a_{i+1,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Note that the elements of the two determinants are exactly the same except for those in row  $i$ .

*Proof:* First use ex. 9, §3; then ex. 8, §3. Then apply the theorem above.

This theorem is useful in evaluating determinants. For, by means of it we can make some elements zero (in fact, all those in any one row or any one column, except possibly for one element in that row or column) without altering the value of the determinant. If we expand a determinant according to a row or column containing zeros, we do not have to evaluate the cofactors of the zero elements.

**Example** Evaluate

$$D = \begin{vmatrix} 2 & 4 & 1 & 4 \\ 2 & -3 & 6 & 1 \\ -1 & 1 & 5 & -1 \\ 1 & -1 & -3 & 2 \end{vmatrix}$$

Alter the third row by adding to its elements the corresponding elements of the fourth row, leaving unchanged all elements not in the third row. Then

$$D = \begin{vmatrix} 2 & 4 & 1 & 4 \\ 2 & -3 & 6 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & -1 & -3 & 2 \end{vmatrix}$$

Now alter the third column by adding to its elements  $-2$  times the corresponding elements of the fourth column, leaving all other elements unchanged. Then

$$D = \begin{vmatrix} 2 & 4 & -7 & 4 \\ 2 & -3 & 4 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & -1 & -7 & 2 \end{vmatrix}$$

If we now expand  $D$  according to the third row, we shall have to evaluate only one cofactor.

### Exercises

#### 1 Evaluate:

a)  $\begin{vmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ -2 & -2 & -3 \end{vmatrix}$

b)  $\begin{vmatrix} 2 & 1 & -4 \\ -3 & -1 & 4 \\ 5 & 7 & 9 \end{vmatrix}$

c)  $\begin{vmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & -4 & -4 \\ 4 & 4 & -3 & -3 \end{vmatrix}$

d)  $\begin{vmatrix} 3 & 2 & -4 \\ 1 & -1 & 1 \\ 2 & 1 & -1 \end{vmatrix}$

e)  $\begin{vmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ -1 & 0 & 0 & 1 \end{vmatrix}$

f)  $\begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 9 \end{vmatrix}$

$$g) \begin{vmatrix} 1-i & 2 & i \\ 1+i & -i & -1 \\ i & 1 & 1+i \end{vmatrix}$$

$$l) \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{vmatrix}$$

$$h) \begin{vmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \\ \omega^2 & 1 & \omega \end{vmatrix} \quad \omega \text{ a cube root of } 1$$

$$m) \begin{vmatrix} 2 & -3 & 4 & -1 \\ 4 & 2 & -1 & 2 \\ 1 & -1 & 2 & 3 \\ 5 & 0 & 3 & 10 \end{vmatrix}$$

$$i) \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{vmatrix}$$

$$n) \begin{vmatrix} 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -3 & 0 \\ 1 & 2 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 & 2 \end{vmatrix}$$

$$j) \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{vmatrix}$$

$$o) \begin{vmatrix} 1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \end{vmatrix}$$

$$k) \begin{vmatrix} 1 & 1 & 1 & 2 \\ 2 & 2 & 3 & 3 \\ 3 & 4 & -4 & -4 \\ 4 & 3 & -3 & -3 \end{vmatrix}$$

**2 Prove:**

$$a) \begin{vmatrix} 1 & x & y+z \\ 1 & y & x+z \\ 1 & z & x+y \end{vmatrix} = 0$$

$$b) \begin{vmatrix} 1 & x & -y \\ -x & 1 & z \\ y & -z & 1 \end{vmatrix} = x^2 + y^2 + z^2 + 1$$

$$c) \begin{vmatrix} y+z & x+z & x+y \\ 3 & 2 & 1 \\ 1 & 2 & 3 \end{vmatrix} = 2 \begin{vmatrix} x & y & z \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{vmatrix}$$

$$d) \begin{vmatrix} a+b & c-d & 1 \\ a-b & c+d & 1 \\ 2a+b & c-2d & 1 \end{vmatrix} = 2d(b-a)$$

$$e) \begin{vmatrix} x & x^2 & 2x^2-3x+1 \\ 1 & x & 2x-3 \\ x-1 & 1 & -3x+5 \end{vmatrix} = 1+x-x^2$$

$$f) \begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = (af - be + cd)^2$$

**3** Solve for  $x$ :

$$\text{a) } \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & x & 2 & 3 \\ 1 & x^2 & 4 & 9 \\ 1 & x^3 & 8 & 27 \end{vmatrix} = 0$$

$$\text{b) } \begin{vmatrix} x & 1 & 1 & 0 \\ 0 & x & 1 & 1 \\ x & -1 & 1 & 0 \\ 0 & x & -1 & 1 \end{vmatrix} = 0$$

$$\text{c) } \begin{vmatrix} 1 & 1 & -1 & 0 \\ 1 & x+1 & x & x \\ 1 & 2x+1 & 3x+1 & 4x+1 \\ 1 & 3x+1 & 6x+2 & 10x+3 \end{vmatrix} = 0$$

**4** Prove without actual calculation:

$$\begin{vmatrix} 0 & a_{12} & a_{13} & a_{14} & a_{15} \\ -a_{12} & 0 & a_{23} & a_{24} & a_{25} \\ -a_{13} & -a_{23} & 0 & a_{34} & a_{35} \\ -a_{14} & -a_{24} & -a_{34} & 0 & a_{45} \\ -a_{15} & -a_{25} & -a_{35} & -a_{45} & 0 \end{vmatrix} = 0$$

(Hint: Multiply each row by  $-1$  and compare with original.)**5** Prove:

$$\begin{vmatrix} x_1^3 + ax_1^2 + bx_1 + c & x_1^2 + ax_1 + b & x_1 + a & 1 \\ x_2^3 + ax_2^2 + bx_2 + c & x_2^2 + ax_2 + b & x_2 + a & 1 \\ x_3^3 + ax_3^2 + bx_3 + c & x_3^2 + ax_3 + b & x_3 + a & 1 \\ x_4^3 + ax_4^2 + bx_4 + c & x_4^2 + ax_4 + b & x_4 + a & 1 \end{vmatrix} = \begin{matrix} (x_1 - x_2)(x_1 - x_3) \\ (x_1 - x_1)(x_1 - x_3) \\ (x_2 - x_4)(x_3 - x_1) \end{matrix}$$

(Hint: Use factor theorem.)

**6** Prove: If  $a_{ni} = \lambda_1 a_{1i} + \lambda_2 a_{2i} + \cdots + \lambda_{n-1,i}$  ( $i = 1, 2, \dots, n$ ), then

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = 0$$

**7** Prove: If the elements of one column are altered by adding to them  $\lambda_1$  times the corresponding elements of a second column and  $\lambda_2$  times the corresponding elements of a third column, all elements not in that one column remaining unaltered, the value of the determinant is unchanged. Extend this result.



8 Prove:

$$a) \begin{vmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1+1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1+2 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1+3 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1+n \end{vmatrix} = n!$$

$$b) \begin{vmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 2 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 2 \end{vmatrix} = n+1, \text{ the determinant being of order } n.$$

$$c) \begin{vmatrix} x & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & x & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & -1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & x & -1 \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_3 & a_2 & x + a_1 \end{vmatrix} \equiv \begin{matrix} x^n + a_1 x^{n-1} \\ + \cdots \\ + a_{n-1} x + a_n \end{matrix}$$

9 Prove:

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 0 \\ a_{n+1,1} & \cdots & a_{n+1,n} & a_{n+1,n+1} & \cdots & a_{n+1,n+m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n+m,1} & \cdots & a_{n+m,n} & a_{n+m,n+1} & \cdots & a_{n+m,n+m} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} a_{n+1,n+1} & \cdots & a_{n+1,n+m} \\ \vdots & \ddots & \vdots \\ a_{n+m,n+1} & \cdots & a_{n+m,n+m} \end{vmatrix}$$

\*10 Prove: If each of the elements in row (or column)  $i$  is multiplied by the cofactor of the corresponding element in row (or column)  $j$ , where  $i \neq j$ , the sum of the products is zero.

11 If each of the  $a_{ij}$  is a polynomial in  $x$ , show that the derivative of

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

is

$$\begin{vmatrix} a'_{11} & a'_{12} & a'_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a'_{21} & a'_{22} & a'_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a'_{31} & a'_{32} & a'_{33} \end{vmatrix}$$

Show also how the derivative may be obtained by differentiating in columns. Extend these results to determinants of any order.

**12** Prove: If  $a$  and  $b$  are rational and

$$\begin{vmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & a & b & 0 \\ 0 & 1 & a & b \end{vmatrix} = 0$$

then  $a = b = 1$ . (Hint: Show that if  $a - 1 \neq 0$  then  $(b - 1)/(a - 1)$  is a rational root of  $x^2 - x + 1 = 0$ .)

**8. Product of determinants** If  $A$  and  $B$  are determinants of order  $n$  with elements  $a_{ij}$  and  $b_{ij}$  respectively, it is often desirable to express  $AB$  as a single determinant of the same order. Let

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} \quad (i = 1, 2, \dots, n; j = 1, 2, \dots, n)$$

so that  $c_{ij}$  is the sum of the products of the elements in the  $i$ th row of  $A$  and the elements in the  $j$ th column of  $B$ . Let  $C$  be the determinant whose elements are  $c_{ij}$ . We show:

#### THEOREM

$$C = AB$$

*Proof:* For simplicity, let  $n = 3$  (although the proof is perfectly general). Then

$$C = \begin{vmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{vmatrix}$$

Expanding  $C$ , we obtain (§3)

$$C = \sum \pm (a_{11}b_{1j_1} + a_{12}b_{2j_1} + a_{13}b_{3j_1})(a_{21}b_{1j_2} + a_{22}b_{2j_2} + a_{23}b_{3j_2})(a_{31}b_{1j_3} + a_{32}b_{2j_3} + a_{33}b_{3j_3})$$

where  $j_1, j_2, j_3$  are the integers 1, 2, 3 in some order (the summation extending over all possible such terms). Each of these products, when multiplied out, is a sum of terms of the form  $a_{1i_1}a_{2i_2}a_{3i_3}b_{1j_1}b_{2j_2}b_{3j_3}$ . Thus, multiplying out each of the products and collecting terms involving like products of  $a$ 's, we obtain for  $C$  a sum of terms of the type  $P_{i_1i_2i_3}a_{1i_1}a_{2i_2}a_{3i_3}$ , where  $P_{i_1i_2i_3}$  is an expression involving only the

$b$ 's (and no  $a$ 's) and  $i_1, i_2, i_3$  may have any of the values 1, 2, 3 (not necessarily distinct).

Since the  $P$ 's do not involve the  $a$ 's, their values are the same for all values of the  $a$ 's. To determine a specific  $P_{i_1 i_2 i_3}$ , say  $P_{k_1 k_2 k_3}$ , let  $a_{1k_1} = a_{2k_2} = a_{3k_3} = 1$  and let all other  $a$ 's equal zero. In the expression  $C = \sum P_{i_1 i_2 i_3} a_{1i_1} a_{2i_2} a_{3i_3}$  every term becomes zero except the one for which  $i_1 = k_1, i_2 = k_2, i_3 = k_3$ , and we obtain  $C = P_{k_1 k_2 k_3}$ . On the other hand, returning to the original form for  $C$  as a determinant, we see that  $C$  has become

$$\begin{vmatrix} b_{k_1 1} & b_{k_1 2} & b_{k_1 3} \\ b_{k_2 1} & b_{k_2 2} & b_{k_2 3} \\ b_{k_3 1} & b_{k_3 2} & b_{k_3 3} \end{vmatrix}$$

Thus,  $P_{k_1 k_2 k_3}$  is this determinant

If any two of  $k_1, k_2, k_3$  are equal, two rows of this determinant are identical, so that  $P_{i_1 i_2 i_3} = 0$  (§7). If  $k_1, k_2, k_3$  are all distinct, this determinant is obtainable from  $B$  by interchanging rows of  $B$  a sufficient number of times; since the interchange of two rows of a determinant merely changes its sign (§7),  $P_{i_1 i_2 i_3} = \pm B$ .

Thus, disregarding the  $P_{i_1 i_2 i_3}$  which equal zero, we have  $C = \sum \pm B a_{1i_1} a_{2i_2} a_{3i_3} = QB$ , where  $Q$  is an expression involving only the  $a$ 's (and no  $b$ 's).

To determine  $Q$  let  $b_{11} = b_{22} = b_{33} = 1$  and all other  $b$ 's equal zero. Then  $B = 1$ , so that  $C = Q$ . On the other hand,

$$C = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = A$$

Hence,  $Q = A$ . Thus,  $C = AB$ , and the theorem is proved.

*Example* Let  $A$  be a determinant of order  $n \geq 2$  with elements  $a_{ij}$ . Let  $A_{ij}$  be the cofactor of  $a_{ij}$ . The determinant  $D$  with elements  $A_{ij}$  is called the adjoint of  $A$ . Prove:  $AD = A^n$ .

$$\begin{aligned} AD &= \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \begin{vmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \cdots & A_{nn} \end{vmatrix} \\ &= \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} \begin{vmatrix} A_{11} & \cdots & A_{n1} \\ \vdots & \ddots & \vdots \\ A_{1n} & \cdots & A_{nn} \end{vmatrix} \quad \text{(by interchanging rows} \\ &\hspace{15em} \text{and columns of } D) \end{aligned}$$

$$\begin{aligned}
&= \begin{vmatrix} a_{11}A_{11} + \cdots + a_{1n}A_{1n} & \cdots & a_{11}A_{n1} + \cdots + a_{1n}A_{nn} \\ \vdots & \ddots & \vdots \\ a_{n1}A_{11} + \cdots + a_{nn}A_{1n} & \cdots & a_{n1}A_{n1} + \cdots + a_{nn}A_{nn} \end{vmatrix} \\
&= \begin{vmatrix} A & 0 & \cdots & 0 & 0 \\ 0 & A & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & A & 0 \\ 0 & 0 & \cdots & 0 & A \end{vmatrix} \quad (\text{by §4 and ex. 10, §7}) \\
&= A^n
\end{aligned}$$

### Exercises

1 Express as a single determinant:

$$a) \begin{vmatrix} 3 & -1 & 4 \\ 0 & -2 & 1 \\ -1 & 2 & 2 \end{vmatrix} \begin{vmatrix} 4 & 0 & 3 \\ 1 & -1 & 0 \\ 1 & 1 & 2 \end{vmatrix}$$

$$b) \begin{vmatrix} 1 & 0 & 3 & 2 & 1 & 0 \\ 2 & 1 & 2 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 2 & 3 \end{vmatrix} \quad c) \begin{vmatrix} 0 & 1 & -1 & 2 \\ 1 & 0 & -2 & 3 \\ -1 & -2 & 0 & 4 \\ 2 & 3 & 4 & 0 \end{vmatrix} \begin{vmatrix} -1 & 3 & 3 & 1 \\ 2 & 1 & -4 & 4 \\ 2 & -1 & 0 & 2 \\ 0 & -1 & 2 & -1 \end{vmatrix}$$

$$2 \text{ Show that } \begin{vmatrix} 1 & 1 & 1^2 \\ x & 1 & -1 \\ x^2 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 3 & x & x^2 + 2 \\ r & x^2 + 2 & x^3 \\ x^2 + 2 & x^3 & x^4 + 2 \end{vmatrix}$$

3 A determinant of order  $n$  with elements  $a_{ij}$  is called orthogonal if  $a_{i,j+1} + a_{i+1,j} + \cdots + a_{i+n,j+n} = 0$  whenever  $i \neq j$  and 1 whenever  $i = j$ . Show that an orthogonal determinant equals  $\pm 1$ .

4 Prove:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} = \begin{vmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} & a_{21}b_{13} + a_{22}b_{23} \\ \lambda b_{11} + \mu b_{21} + b_{31} & \lambda b_{12} + \mu b_{22} + b_{32} & \lambda b_{13} + \mu b_{23} + b_{33} \end{vmatrix}$$

for all values of  $\lambda$  and  $\mu$ .

9. Rank of matrix As in §2, we define an  $m$  by  $n$  matrix (where  $m$  may or may not equal  $n$ ) as a rectangular array of  $mn$  numbers or variables

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

arranged in  $m$  rows and  $n$  columns.

If  $m$  and  $n$  are unequal, there is no determinant of the matrix, since a determinant must have as many rows as columns. However, by omitting some rows or columns, certain determinants associated with the matrix can be formed.

If  $1 \leq i_1 < i_2 < \cdots < i_k \leq m$  and  $1 \leq j_1 < j_2 < \cdots < j_k \leq n$ , where the  $i$ 's and  $j$ 's are integers, the determinant of order  $k$

$$\begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \cdots & a_{i_1 j_k} \\ a_{i_2 j_1} & a_{i_2 j_2} & \cdots & a_{i_2 j_k} \\ \cdot & \cdot & \cdots & \cdot \\ a_{i_k j_1} & a_{i_k j_2} & \cdots & a_{i_k j_k} \end{vmatrix}$$

is called a  $k$ -rowed minor of the matrix. Thus, a  $k$ -rowed minor is a determinant whose elements are the elements of the matrix which appear in any  $k$  rows and any  $k$  columns, the order of the rows and columns being the same in the determinant as in the matrix.

If there exists a  $k$ -rowed minor which is not zero, while every minor of order higher than  $k$  is zero, the matrix is said to be of rank  $k$  (or to have rank  $k$ ). We also say the rank of the matrix is  $k$ .

If the matrix has no minor which is different from zero, the rank of the matrix is said to be zero. If the rank is zero, every one-rowed minor, i.e., every element, is zero. Conversely, if every element is zero, the rank is zero.

*Example* Determine the rank of

$$\begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 2 & -2 & 4 \\ 1 & 1 & 0 & 7 \end{pmatrix}$$

There are four three-rowed minors

$$\begin{vmatrix} 1 & -1 & 2 \\ 0 & 2 & -2 \\ 1 & 1 & 0 \end{vmatrix}, \begin{vmatrix} 1 & -1 & 3 \\ 0 & 2 & 4 \\ 1 & 1 & 7 \end{vmatrix}, \begin{vmatrix} 1 & 2 & 3 \\ 0 & -2 & 4 \\ 1 & 0 & 7 \end{vmatrix}, \begin{vmatrix} -1 & 2 & 3 \\ 2 & -2 & 4 \\ 1 & 0 & 7 \end{vmatrix}$$

and each is zero.

The two-rowed minor  $\begin{vmatrix} 1 & -1 \\ 0 & 2 \end{vmatrix}$  in the upper left-hand corner is non-zero. Thus, the rank of the matrix is two.

To determine the rank of a matrix it may be necessary to evaluate a great many determinants. There are, however, many theorems by means of which the computation involved may be greatly lessened. We state and prove only one fairly obvious theorem.

### THEOREM

*If some  $k$ -rowed minor of a matrix is non-zero while every  $(k + 1)$ -rowed minor is zero, the rank of the matrix is  $k$ .*

*Proof:* We must show that every minor of order higher than  $k$  vanishes.

By hypothesis every  $(k + 1)$ -rowed minor vanishes.

Any  $(k + 2)$ -rowed minor is the sum of the products of the elements in one row and their cofactors (§4). The cofactors are, except possibly for sign,  $(k + 1)$ -rowed minors. Therefore, all the cofactors are zero. Hence, the  $(k + 2)$ -rowed minors vanish.

In the same way, every  $(k + 3)$ -rowed minor vanishes. Continuing this line of reasoning, we see that every minor whose order exceeds  $k$  is zero.

*Example* Show that the rank of  $\begin{pmatrix} 1 & 4 & -1 & 2 \\ 2 & 8 & -2 & 4 \\ -1 & -4 & 1 & -2 \end{pmatrix}$  is one.

There is a one-rowed minor which is not zero while each of the 18 two-rowed minors is zero. It is not necessary to evaluate the four three-rowed minors.

If we make use of the result in exercise 10 below, we can see more easily that the rank of this matrix is one. For, if we add to the elements in the first row the corresponding elements in the third

row, we obtain  $\begin{pmatrix} 0 & 0 & 0 & 0 \\ 2 & 8 & -2 & 4 \\ -1 & -4 & 1 & -2 \end{pmatrix}$  with the same rank as the

given matrix. If we now add to the elements in the second row twice the corresponding elements in the third row, we obtain

$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & -4 & 1 & -2 \end{pmatrix}$ , which again has the same rank as the given

matrix. The rank of the last matrix is obviously one.

## Exercises

1 Determine the rank of each of the following:

$$a) \begin{pmatrix} 1 & 0 & -2 \\ 2 & -5 & 1 \\ 0 & -5 & 3 \end{pmatrix}$$

$$d) \begin{pmatrix} 2 & -2 & 3 & -3 \\ 0 & 2 & -1 & 1 \\ 2 & 0 & 2 & -2 \end{pmatrix}$$

$$b) \begin{pmatrix} -3 & 1 & -2 & -1 \\ 3 & -4 & -1 & -5 \\ 2 & 0 & 2 & 2 \end{pmatrix}$$

$$e) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

$$c) \begin{pmatrix} 1 & 1+i & i & 1 \\ 1-i & 1 & i & -i \\ i & 1 & 1-i & 2 \end{pmatrix}$$

2 Determine the rank for all possible values of  $x$ :

$$a) \begin{pmatrix} x & -1 & 2 \\ 2 & -2x & 4 \\ -1 & 1 & -2x \end{pmatrix}$$

$$c) \begin{pmatrix} x+2 & 0 & -1 \\ 0 & x+2 & -3 \\ -2 & 1 & x \end{pmatrix}$$

$$b) \begin{pmatrix} x-1 & 1 & 1 \\ 1 & 0 & 1 \\ -1 & -1 & x+1 \end{pmatrix}$$

3 Determine the rank of

$$\begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix}$$

for all values of  $a, b, c$ .

4 Prove: Interchanging two rows (or columns) of a matrix does not change its rank.

5 Prove: If the rank of

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

is  $k$ , then the rank of

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}$$

is  $k$  or  $k+1$ .

6 Prove: If the rows of one matrix are the columns of another, then the two matrices have the same rank.

\*7 Prove:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$$

have the same ranks.

8 From an  $m$ -rowed matrix of rank  $k$ ,  $m - 1$  rows are selected. Show that the  $(m - 1)$ -rowed matrix has rank at least  $k - 1$ .

\*9 Show that

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m-1,1} \\ a_{11}\lambda_1 + a_{21}\lambda_2 + \cdots + a_{m-1,1}\lambda_{m-1} \\ a_{12} \\ a_{22} \\ \vdots \\ a_{m-1,2} \\ a_{12}\lambda_1 + a_{22}\lambda_2 + \cdots + a_{m-1,2}\lambda_{m-1} \\ \vdots \vdots a_{1n} \\ \vdots \vdots a_{2n} \\ \vdots \vdots \vdots \\ \vdots \vdots a_{m-1,n} \\ \vdots \vdots a_{1n}\lambda_1 + a_{2n}\lambda_2 + \cdots + a_{m-1,n}\lambda_{m-1} \end{pmatrix}$$

has rank less than  $m$ .

- 10 Prove: Adding to the elements of one row (or column) a common multiple of the corresponding elements of another row (or column) does not change the rank of a matrix.
- 11 Prove: If  $r$  is the rank of the matrix formed by the elements in the first  $m$  rows of an  $n$ -rowed square matrix, where  $1 \leq m \leq n$ , then the rank of the  $n$ -rowed matrix is  $r + (n - m)$  or less.
- 12 Prove: The rank of

$$\begin{pmatrix} a_1 + b_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_m + b_m & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

does not exceed the rank of either

$$\begin{pmatrix} a_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_m & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} b_1 & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_m & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$



- 13** If  $A$  and  $B$  are square matrices of order  $n$  with elements  $a_{ij}$  and  $b_{ij}$ , respectively, and  $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$  ( $i = 1, 2, \cdots, n$ ;  $j = 1, 2, \cdots, n$ ), the matrix whose elements are  $c_{ij}$  is called the product  $AB$  (compare §8). Prove. The rank of  $AB$  does not exceed the rank of either  $A$  or  $B$ .

## LINEAR EQUATIONS

**1. Linear dependence of constants** If  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n$  are two sets of numbers, we say they are proportional if the ratios  $a_1/b_1, a_2/b_2, \dots, a_n/b_n$  are all equal. This, however, precludes the possibility of any of the  $b$ 's being zero. Hence, a better way to phrase the definition is to say that the two sets are proportional if there exists a  $\lambda$  such that  $a_i = \lambda b_i$  for  $i = 1, 2, \dots, n$ .

Even this, however, is not completely satisfactory since, for example, 0, 0 and 1, 2 would be proportional (with  $\lambda = 0$ ) if  $a_1 = 0, a_2 = 0, b_1 = 1, b_2 = 2$ , but not proportional if  $a_1 = 1, a_2 = 2, b_1 = 0, b_2 = 0$ .

To remedy this, we can say that the two sets are proportional if there exists a  $\lambda$  such that  $a_i = \lambda b_i$  ( $i = 1, 2, \dots, n$ ) or a  $\mu$  such that  $b_i = \mu a_i$  ( $i = 1, 2, \dots, n$ ). This is satisfactory, but cumbersome. Notice, however, that in the first case we have  $c_1 a_i + c_2 b_i = 0$  ( $i = 1, 2, \dots, n$ ) with  $c_1 = 1, c_2 = -\lambda$ , and in the second a similar relationship with  $c_1 = \mu, c_2 = -1$ . In either case, at least one of  $c_1$  and  $c_2$  is non-zero.

Conversely, if such a relationship exists and at least one of  $c_1$  and  $c_2$  is non-zero, then either

(a)  $c_1 \neq 0$ , so that  $a_i = \lambda b_i$  with  $\lambda = -\frac{c_2}{c_1}$ , or

(b)  $c_2 \neq 0$ , so that  $b_i = \mu a_i$  with  $\mu = -\frac{c_1}{c_2}$ .

Thus, we have a convenient and symmetrical way of expressing the proportionality of two sets of numbers. Furthermore, the form of the expression suggests an extension of the concept to three or more sets of constants.

Let  $a_{11}, a_{12}, \dots, a_{1n}$  ( $i = 1, 2, \dots, m$ ) be  $m$  sets of constants,  $n$  in each set. (Each number has two subscripts, the first indicating which set it is in and the second which number in the set it is.) We say the  $m$  sets are linearly dependent if there exist numbers  $c_1, c_2, \dots, c_m$ , not all zero, such that

$$\begin{aligned} c_1 a_{11} + c_2 a_{21} + \dots + c_m a_{m1} &= 0 \\ c_1 a_{12} + c_2 a_{22} + \dots + c_m a_{m2} &= 0 \\ \cdot &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ c_1 a_{1n} + c_2 a_{2n} + \dots + c_m a_{mn} &= 0 \end{aligned}$$

These equations may be written compactly as

$$c_1 a_{1j} + c_2 a_{2j} + \dots + c_m a_{mj} = 0 \quad (j = 1, 2, \dots, n)$$

They express the fact that the  $j$ th numbers of the  $m$  sets are connected by this relation, the numbers  $c_1, c_2, \dots, c_m$  being the same for all values of  $j$ .

We have seen that linear dependence of two sets of constants is nothing but proportionality.

If the  $m$  sets are not linearly dependent, they are said to be linearly independent.

*Example* The three sets  $(2, -2, 4, 3)$ ,  $(0, 1, -2, -3)$ ,  $(4, -5, 10, 9)$ , with four numbers in each set, are linearly dependent, as we can see by taking  $c_1 = 2$ ,  $c_2 = -1$ ,  $c_3 = -1$  as the multipliers. (Here the multipliers are easily guessed; in §2 we shall develop a systematic way of obtaining them.)

*Example* The three sets  $(0, 1, -1)$ ,  $(2, 0, -3)$ ,  $(4, 1, 0)$ , with three numbers in each set, are linearly independent.

For, if  $c_1 a_{1j} + c_2 a_{2j} + c_3 a_{3j} = 0$  for  $j = 1, 2, 3$ , then

$$\begin{aligned} c_1 0 + c_2 2 + c_3 4 &= 0 \\ c_1 1 + c_2 0 + c_3 1 &= 0 \\ c_1 (-1) + c_2 (-3) + c_3 0 &= 0 \end{aligned}$$

Solving these simultaneous equations to find the values of  $c_1, c_2, c_3$ , we find  $c_1 = c_2 = c_3 = 0$ .

## Exercises

- 1 Prove: A single set of numbers is linearly dependent if and only if all the numbers in the set are zero.
- 2 Prove: If among  $m$  sets of numbers there are  $m - 1$  or fewer sets which are linearly dependent, then the  $m$  sets are linearly dependent.
- 3 Determine whether the following sets are linearly dependent:
  - a)  $-2, 3, 1, 0; 1, 4, -4, 2; 5, -2, -6, 2$
  - b)  $1, -2, -1, 2; 3, 4, 2, 1; 8, 4, 2, 6$
  - c)  $1, 1; 2, 3; 3, 5$
  - d)  $1, 0, 0; 0, -2, 0; 0, 0, 4$
  - e)  $-1, 1 + i, 0, 0; i, i, 1, -1; 1 - i, i, -i, i$
  - f)  $1, -1, 2; 2, 3, -4; 3, 2, 2$
  - g)  $3, 4, 1, 0; -1, 2, -2, 1; 1, 8, -3, 1$
- 4 Find all the values of  $k$  for which the following sets are linearly dependent:
  - a)  $k, 1, 1, 1; 1, k, 1, 1; 1, 1, k, 1$
  - b)  $k, 4, 3, -2; 1, k, 2, -2; k + 2, 8, 10, -8$
  - c)  $4, 0, 2, 1; -1, 1, k, 1; 1, 3, 2, k$
  - d)  $0, 1, 2; 3, k, 4; 1, k + 1, -2; 0, k, 0$
  - e)  $1, -k, k - 1, -1; 0, k^2 + 1, 1, k + 1; k, 1, k^2, 1$
  - f)  $-3, 1, k - 1, k; k + 1, 2, -2, 1; 2 - k, 1, k + 3, 1$
- 5 Prove. If the three sets  $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n), (c_1, c_2, \dots, c_n)$  are linearly independent, then the three sets  $(a_1, a_2, \dots, a_n), (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n), (a_1 + b_1 + c_1, a_2 + b_2 + c_2, \dots, a_n + b_n + c_n)$  are also.

**2. Criterion for linear dependence** If  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n, n > 1$ , are proportional, then there is a  $\lambda$  such that  $a_i = \lambda b_i$ , or a  $\mu$  such that  $b_i = \mu a_i$  ( $i = 1, 2, \dots, n$ ). Suppose, to be specific, that  $a_i = \lambda b_i$ . Then, for any two-rowed minor (§9, Ch. 12) of the matrix

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

we have

$$\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} = \begin{vmatrix} \lambda b_i & \lambda b_j \\ b_i & b_j \end{vmatrix} = \lambda \begin{vmatrix} b_i & b_j \\ b_i & b_j \end{vmatrix} = 0$$

Thus, the rank of the matrix is less than two.

Conversely, suppose the rank of the matrix is less than two. Then every two-rowed minor vanishes.

If every  $a_i$  is zero, then  $1a_i + 0b_i = 0$ . Hence the two sets are linearly dependent.

If not every  $a_i$  is zero, suppose, to be specific,  $a_1 \neq 0$ . By hypothesis,

$$\begin{vmatrix} a_1 & a_i \\ b_1 & b_i \end{vmatrix} = 0 \text{ for } i = 2, 3, \dots, n$$

Therefore,  $-b_1a_i + a_1b_i = 0$  for  $i = 2, 3, \dots, n$ . For  $i = 1$  this equality obviously holds. Hence  $c_1a_i + c_2b_i = 0$  ( $i = 1, 2, \dots, n$ ) where  $c_1 = -b_1$ ,  $c_2 = a_1 \neq 0$ . Thus, again we have linear dependence.

This result for two sets of numbers is a special case of the following general result:

#### THEOREM

If  $m \leq n$  the  $m$  sets of  $n$  constants  $a_{11}, a_{12}, \dots, a_{1n}$  ( $i = 1, 2, \dots, m$ ) are linearly dependent if and only if the rank of the matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \dots & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

is less than  $m$ .

*Proof:* Suppose the  $m$  sets linearly dependent. Then

$$c_1a_{1j} + c_2a_{2j} + \dots + c_ma_{mj} = 0 \quad (j = 1, 2, \dots, n)$$

with at least one of the  $c$ 's different from zero.

We may and do suppose, for convenience, that  $c_m \neq 0$ . For, if  $c_m = 0$  but  $c_i \neq 0$  where  $i \neq m$ , we may rearrange the  $m$  rows so that the  $i$ th row becomes the last.

Since  $c_m \neq 0$ , we obtain from the preceding equations

$$a_{mj} = \lambda_1 a_{1j} + \lambda_2 a_{2j} + \dots + \lambda_{m-1} a_{m-1,j} \quad (j = 1, 2, \dots, n)$$

where  $\lambda_1 = -\frac{c_1}{c_m}$ ,  $\lambda_2 = -\frac{c_2}{c_m}$ ,  $\dots$ ,  $\lambda_{m-1} = -\frac{c_{m-1}}{c_m}$ .

The matrix may now be rewritten as

$$\left( \begin{array}{cccc}
 a_{11} & & & \\
 a_{21} & & & \\
 \cdot & & & \\
 a_{m-1,1} & & & \\
 \lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{m-1} a_{m-1,1} & & & \\
 & a_{12} & & \cdots \\
 & a_{22} & & \cdots \\
 & \cdot & & \cdots \\
 & a_{m-1,2} & & \cdots \\
 & \lambda_1 a_{12} + \lambda_2 a_{22} + \cdots + \lambda_{m-1} a_{m-1,2} & & \cdots \\
 & & a_{1n} & \\
 & & a_{2n} & \\
 & & \cdot & \\
 & & a_{m-1,n} & \\
 & & \lambda_1 a_{1n} + \lambda_2 a_{2n} + \cdots + \lambda_{m-1} a_{m-1,n} & 
 \end{array} \right)$$

By ex. 9, §9, Ch. 12, the rank of the matrix is less than  $m$ . Hence, one part of the theorem is proved.

To establish the converse, suppose the rank of the matrix is less than  $m$ .

If the rank is zero then all the  $a_{ij}$  are zero (§9, Ch. 12) and we obviously have linear dependence.

Suppose the rank is  $k$  where  $0 < k < m$ . Then some  $k$ -rowed minor is non-zero. We can rearrange the rows and columns of the matrix, if necessary, so that a  $k$ -rowed minor which is non-zero is in the upper left-hand corner. Hence, for convenience, we suppose

$$\begin{vmatrix} a_{11} & \cdots & a_{1k} \\ \cdot & \cdots & \cdot \\ a_{k1} & \cdots & a_{kk} \end{vmatrix} \neq 0$$

We show first that the first  $k+1$  rows of the matrix are linearly dependent.

Since the matrix is of rank  $k$ , every  $(k+1)$ -rowed minor vanishes. In particular, every  $(k+1)$ -rowed minor obtained by adding row  $k+1$  and any one column to the  $k$ -rowed minor in the upper left-hand corner is zero. That is,

$$\begin{vmatrix} a_{11} & \cdots & a_{1k} & a_{1j} \\ \cdot & \cdots & \cdot & \cdot \\ a_{k1} & \cdots & a_{kk} & a_{kj} \\ a_{k+1,1} & \cdots & a_{k+1,k} & a_{k+1,j} \end{vmatrix} = 0 \quad \text{for } j = k+1, k+2, \cdots, n$$

For  $j = 1, 2, \dots, k$  this determinant has two identical columns and, therefore, is zero (§7, Ch. 12). Hence, the determinant is zero for all values of  $j$  from 1 to  $n$  inclusive.

In this determinant the cofactors of the elements in the last column do not depend upon the value of  $j$ . Hence, expanding the determinant according to the last column (§5, Ch. 12),

$$c_1 a_{1j} + c_2 a_{2j} + \dots + c_{k+1} a_{k+1j} = 0 \quad \text{for } j = 1, 2, \dots, n,$$

where  $c_1, c_2, \dots, c_{k+1}$  are numbers independent of  $j$ . In particular,  $c_{k+1}$ , the cofactor of  $a_{k+1,1}$ , is the determinant of order  $k$  in the upper left-hand corner of the matrix, which is different from zero.

Therefore, the first  $k+1$  rows of the matrix are linearly dependent.

If  $k+1 = m$ , there is nothing more to be proved. If  $k+1 < m$ , we may take  $c_{k+2} = c_{k+3} = \dots = c_m = 0$ .

*Remark 1* Looking over the proof of the second part, we can see that we have shown the following: Suppose  $m \leq n$  and that some  $k$ -rowed minor,  $k < m$ , is non-zero. Consider any  $k+1$  rows of the matrix which contain the rows of this minor, and suppose that in this  $(k+1)$ -rowed matrix every  $(k+1)$ -rowed minor which contains the given minor is zero. Then the  $k+1$  rows are linearly dependent.

*Remark 2* Note that the proof of the theorem supplies a method for obtaining the multipliers  $c_1, c_2, \dots, c_m$ .

### THEOREM

*If  $m > n$  any  $m$  sets of  $n$  numbers are linearly dependent.*

*Proof:* Let  $a_{i1}, a_{i2}, \dots, a_{in}$  ( $i = 1, 2, \dots, m$ ),  $m > n$ , be given constants. Add  $m - n$  zeros to each set, obtaining the  $m$  sets  $a_{i1}, a_{i2}, \dots, a_{in}, 0, \dots, 0$  ( $i = 1, 2, \dots, m$ ) with  $m$  numbers in each set.

The matrix formed by these numbers is an  $m$ -rowed square matrix with at least one column of zeros. The determinant of the matrix is zero. Therefore, the rank of the matrix is less than  $m$ .

By the preceding theorem, the rows of the matrix are linearly dependent, which proves the theorem.

**Example** Show that the three sets  $(3, 0, 1, 4, 9)$ ,  $(0, -1, 2, 0, 3)$ ,  $(2, -2, 1, -1, 6)$  are linearly independent.

The matrix

$$\begin{pmatrix} 3 & 0 & 1 & 4 & 9 \\ 0 & -1 & 2 & 0 & 3 \\ 2 & -2 & 1 & -1 & 6 \end{pmatrix}$$

has rank three, since

$$\begin{vmatrix} 3 & 0 & 4 \\ 0 & -1 & 0 \\ 2 & -2 & -1 \end{vmatrix} = 11 \neq 0$$

**Example** Show that the four sets  $(5, 2, -2, -1, 1)$ ,  $(3, 1, -2, 1, 0)$ ,  $(1, 1, 2, -5, 2)$ ,  $(2, -2, 4, 6, 9)$  are linearly dependent.

Consider the matrix  $\begin{pmatrix} 5 & 2 & -2 & -1 & 1 \\ 3 & 1 & -2 & 1 & 0 \\ 1 & 1 & 2 & -5 & 2 \\ 2 & -2 & 4 & 6 & 9 \end{pmatrix}$

The minor  $\begin{vmatrix} 5 & 2 \\ 3 & 1 \end{vmatrix} = -1 \neq 0$

appears in the first two rows.

The minors in the first three rows which contain this minor are

$$\begin{vmatrix} 5 & 2 & -2 \\ 3 & 1 & -2 \\ 1 & 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 5 & 2 & -1 \\ 3 & 1 & 1 \\ 1 & 1 & -5 \end{vmatrix}, \quad \begin{vmatrix} 5 & 2 & 1 \\ 3 & 1 & 0 \\ 1 & 1 & 2 \end{vmatrix}$$

and each of these is zero.

By *Remark 1* above, the first three sets (and, therefore, all four) are linearly dependent.

We may take  $c_4 = 0$  and for  $c_1, c_2, c_3$  the cofactors of the elements in the last column of any one of the three-rowed minors above. Thus,

$$c_1 = \begin{vmatrix} 3 & 1 \\ 1 & 1 \end{vmatrix} = 2, \quad c_2 = -\begin{vmatrix} 5 & 2 \\ 1 & 1 \end{vmatrix} = -3, \quad c_3 = \begin{vmatrix} 5 & 2 \\ 3 & 1 \end{vmatrix} = -1$$

### Exercises

**1** Show that the following sets are linearly dependent and find multipliers  $c_i$ :



- a) 2, -1, 1; 3, -2, 4; -1, 1, -3  
 b) 3, 2, 2, -1; 3, 1, -1, 1; 3, 5, 11, -7  
 c) 1, 4, 3, -1, 2; -2, 1, -3, 4, 1; -8, -5, -15, 14, -1  
 d) -7, 1, 1, 4; 3, 3, 2, -5; 6, -8, 3, 0; -14, 16, 3, -2  
 e) -2, 1, 0, -1, 4; 1, 3, -4, 1, 2; 5, -1, 1, -5, 2; -2, 8, -8, 0, 12
- 2 Show that the following sets are linearly independent:  
 a) 2, 1, 5, 6, 1; 0, 4, 7, -9, -5; 0, 0, -3, 2, 6  
 b) 1, 2, -1, 0; 1, 2, -1, 3; 3, 6, -2, 0  
 c) 3, 0, 1; -1, 4, 2; 0, 5, 7  
 d) 2, 1, -1, 1; 0, -1, 3, -4; 5, 6, -2, 3; 1, -2, 2, 1
- 3 Determine all the values of  $k$  for which the following sets are linearly dependent, and for these values of  $k$  find multipliers  $c_i$ :  
 a) 1, 1, 1; 1,  $k+1$ , 1; 1, 1,  $k$   
 b) 1, 1,  $k$ ; 1, 1, 1; 2,  $k$ , 2  
 c)  $k-2$ ,  $2k$ ,  $2k$ ; 2,  $-k$ , 2, 2,  $-k$   
 d) 0,  $k+1$ , 1,  $k$ ;  $k+1$ , 0,  $k$ , 1; 1,  $k$ , 0,  $k+1$   
 e) -2, 0, -1, 2; 0, 2,  $-a$ ,  $-k$ ;  $k$ , -2,  $a$ , 0  
 f) 1, -1,  $k$ ,  $a$ ; 1, 0,  $k$ ,  $k+a$ ; 1, 1,  $k+1$ ,  $2k+1$   
 g) 1, -1, 2,  $k$ ;  $k$ , 0,  $k+1$ ,  $-k$ ;  $k-2$ , 2,  $k-3$ ,  $-3k$   
 h) 2,  $k$ ,  $-2k$ , 3; -1,  $k$ , 3,  $-3k$ ; 1, 5, 5, -3  
 i)  $k^2$ , 1,  $k$ , 1;  $-k$ , -1, 0,  $k-1$ ; -1, -1, 1,  $k$
- 4 Prove: If  $a_{i1}, a_{i2}, \dots, a_{in}$  ( $i=1, 2, \dots, m$ ),  $m > 1$ , are linearly independent, then  $a_{i1}, a_{i2}, \dots, a_{in}$  ( $i=1, 2, \dots, m-1$ ) and  $ca_{11} + a_{m1}, ca_{12} + a_{m2}, \dots, ca_{1n} + a_{mn}$  are linearly independent.
- 5 Prove: If  $m \leq n$  and the rank of

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

is less than  $m-1$ , then there are two sets of numbers  $c_1, c_2, \dots, c_m$  and  $c'_1, c'_2, \dots, c'_m$  which are not proportional such that

$$c_1 a_{1j} + c_2 a_{2j} + \dots + c_m a_{mj} = 0, \quad c'_1 a_{1j} + c'_2 a_{2j} + \dots + c'_m a_{mj} = 0 \\ (j=1, \dots, n)$$

3. Linear equations A system of equations of the form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

where the  $a_i$  and  $b_j$  ( $i = 1, 2, \dots, m; j = 1, 2, \dots, n$ ) are given numbers and  $x_1, x_2, \dots, x_n$  are numbers which may or may not be known, is called a system of  $m$  linear equations in  $x_1, x_2, \dots, x_n$ .

Generally, the  $x$ 's are unknowns which are to be determined. The system is then referred to as a system of  $m$  linear equations in  $n$  unknowns. It is not necessary that  $m = n$ .

A solution of the system is a set of  $n$  numbers ( $\lambda_1, \lambda_2, \dots, \lambda_n$ ) such that every equation in the system becomes a true statement of equality when we simultaneously replace  $x_1$  by  $\lambda_1, x_2$  by  $\lambda_2, \dots, x_n$  by  $\lambda_n$ . Such a set of numbers is said to satisfy the equations.

To solve the system means to find all the solutions.

*Example 1* Solve the system of three equations in the unknowns  $x, y, z$ :

$$\begin{array}{rcl} x - y + 2z & = & 4 \\ 2x + y - z & = & 3 \\ 3x & + & z = 5 \end{array}$$

Let  $(x, y, z)$  be a solution, if there is one. From the first two equations, by adding left sides and right sides,  $3x + z = 7$ . But this contradicts the third of the given equations. Hence, there is no solution.

*Example 2* Solve the system

$$\begin{array}{rcl} x - y + 2z & = & 4 \\ 2x + y - z & = & 3 \\ 4x - y + 3z & = & 11 \end{array}$$

As in example 1, if  $(x, y, z)$  is a solution, then  $3x + z = 7$ . Thus, a solution, if there is one, must have the form  $(x, y, 7 - 3x)$ .

To see if any such set of numbers is a solution, we substitute directly into the given equations. From the first equation we then find, after simplification,  $y = 10 - 5x$ . Thus, the only possible solutions are of the form  $(x, 10 - 5x, 7 - 3x)$ .

Direct substitution shows that every such set of numbers, regardless of what value  $x$  may have, satisfies all three of the given equations.

Thus, there are infinitely many solutions and every solution is obtainable by letting  $x$  have a specific value in  $(x, 10 - 5x, 7 - 3x)$ .

**Example 3** Find all the solutions of the system

$$\begin{aligned}x - y + 2z &= 4 \\2x + y - z &= 3 \\4x - y + 4z &= 9\end{aligned}$$

If  $(x, y, z)$  is a solution, from the first two equations we obtain by addition  $3x + z = 7$  and from the last two, in a similar way,  $2x + z = 4$ . From these two equations in  $x$  and  $z$  we obtain by subtraction  $x = 3$ .

Letting  $x = 3$  in  $2x + z = 4$ , we have  $z = -2$ .

Letting  $x = 3, z = -2$  in the first of the given equations, we have  $y = -5$ . Thus,  $(3, -5, -2)$  is the only possible solution. Direct substitution shows that it does actually satisfy all the given equations. Hence, the given system has one and only one solution.

**4. Cramer's rule** In view of the preceding examples we naturally inquire: Under what conditions does a system of linear equations have solutions, and how can they be obtained? To discuss the general situation we first consider the special case when  $m = n$  and the determinant of the system

$$D = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

is different from zero. In this case we show that there is always a unique solution and it can be obtained by a method known as Cramer's rule.

In each of the examples of §3 we have  $m = n$ . The determinants of the systems are

$$\begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & -1 \\ 3 & 0 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & -1 \\ 4 & -1 & 3 \end{vmatrix} = 0, \quad \begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & -1 \\ 4 & -1 & 4 \end{vmatrix} = 3$$

respectively. Thus, Cramer's rule can be applied only in example 3, and we did see that in this example there is a unique solution.

To establish Cramer's rule, consider the  $n$  linear equations in  $n$  unknowns

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i \quad (i = 1, 2, \cdots, n)$$

where  $D \neq 0$ .

Let  $(x_1, x_2, \dots, x_n)$  be a solution, if there is one.

Let  $A_{ij}$  be the cofactor of  $a_{ij}$  in  $D$ .

Let  $j$  be a fixed integer between 1 and  $n$  inclusive. Multiply both sides of the  $i$ th equation by  $A_{ij}$  and then add the right sides and the left sides of the equations for  $i = 1, 2, \dots, n$ . We obtain

$$\begin{aligned} A_{1j}(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n) + A_{2j}(a_{21}x_1 + a_{22}x_2 + \dots \\ + a_{2n}x_n) + \dots + A_{nj}(a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n) \\ = A_{1j}b_1 + A_{2j}b_2 + \dots + A_{nj}b_n \end{aligned}$$

Regrouping the terms on the left side, we have

$$\begin{aligned} (a_{11}A_{1j} + a_{21}A_{2j} + \dots + a_{n1}A_{nj})x_1 + (a_{12}A_{1j} + a_{22}A_{2j} + \dots \\ + a_{n2}A_{nj})x_2 + \dots + (a_{1n}A_{1j} + a_{2n}A_{2j} + \dots + a_{nn}A_{nj})x_n \\ = A_{1j}b_1 + A_{2j}b_2 + \dots + A_{nj}b_n \end{aligned}$$

In this equation the coefficient of  $x_i$  is the sum of the products of the elements in column  $i$  of  $D$  by the cofactors of the corresponding elements in column  $j$ . Hence, when  $i \neq j$  the coefficient of  $x_i$  is zero (ex. 10, §7, Ch. 12) while the coefficient of  $x_j$  is  $D$  (§5, Ch. 12).

Thus, the preceding equation is

$$Dx_j = A_{1j}b_1 + A_{2j}b_2 + \dots + A_{nj}b_n \quad (j = 1, 2, \dots, n)$$

Since  $D \neq 0$ ,

$$x_j = \frac{A_{1j}}{D}b_1 + \frac{A_{2j}}{D}b_2 + \dots + \frac{A_{nj}}{D}b_n \quad (j = 1, 2, \dots, n)$$

These equations determine  $(x_1, x_2, \dots, x_n)$  uniquely, which means that there cannot be more than one solution.

To verify that this one possible solution actually is a solution, substitute the expressions found for  $x_1, x_2, \dots, x_n$  into the equations of the given system. The left side of the  $i$ th equation becomes

$$\begin{aligned} a_{i1}x_1 + a_{i2}x_2 + \dots + a_{in}x_n \\ = a_{i1} \left( \frac{A_{11}}{D}b_1 + \frac{A_{21}}{D}b_2 + \dots + \frac{A_{n1}}{D}b_n \right) + \\ a_{i2} \left( \frac{A_{12}}{D}b_1 + \frac{A_{22}}{D}b_2 + \dots + \frac{A_{n2}}{D}b_n \right) + \dots + \\ a_{in} \left( \frac{A_{1n}}{D}b_1 + \frac{A_{2n}}{D}b_2 + \dots + \frac{A_{nn}}{D}b_n \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{D} (a_{11}A_{11} + a_{12}A_{12} + \cdots + a_{1n}A_{1n})b_1 + \\
&\quad \frac{1}{D} (a_{21}A_{21} + a_{22}A_{22} + \cdots + a_{2n}A_{2n})b_2 + \cdots + \\
&\quad \frac{1}{D} (a_{n1}A_{n1} + a_{n2}A_{n2} + \cdots + a_{nn}A_{nn})b_n
\end{aligned}$$

The coefficient of  $b_i$  is  $(1/D)(a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in})$  ( $j = 1, 2, \dots, n$ ). The factor in the long parentheses is the sum of the products of the elements in row  $i$  of  $D$  by the cofactors of the corresponding elements in row  $j$ . Hence, this factor is zero when  $j \neq i$  and  $D$  when  $j = i$ . Thus,

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1$$

which shows that the values of  $x_1, x_2, \dots, x_n$  satisfy all the equations of the given system.

Now let us examine more closely the expression for  $x_1$ .

We know (§ 5, Ch. 12) that

$$A_{1j}a_{1j} + A_{2j}a_{2j} + \cdots + A_{nj}a_{nj} = D$$

$A_{1j}, A_{2j}, \dots, A_{nj}$  are, except possibly for sign, certain determinants of order  $n - 1$  obtained from  $D$  by deleting column  $j$  and, in each case, some one row. Therefore, they are independent of  $a_{1j}, a_{2j}, \dots, a_{nj}$ . Hence  $A_{1j}b_1 + A_{2j}b_2 + \cdots + A_{nj}b_n$  is what  $A_{1j}a_{1j} + A_{2j}a_{2j} + \cdots + A_{nj}a_{nj}$  becomes when in the latter, we replace  $a_{1j}$  by  $b_1, a_{2j}$  by  $b_2, \dots, a_{nj}$  by  $b_n$ . Therefore,  $A_{1j}b_1 + A_{2j}b_2 + \cdots + A_{nj}b_n$  is what  $D$  becomes when in  $D$  we replace the elements  $a_{1j}, a_{2j}, \dots, a_{nj}$  by  $b_1, b_2, \dots, b_n$  respectively. That is,

$$\begin{aligned}
&A_{1j}b_1 + A_{2j}b_2 + \cdots + A_{nj}b_n \\
&= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1, j-1} & b_1 & a_{1, j+1} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2, j-1} & b_2 & a_{2, j+1} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{n, j-1} & b_n & a_{n, j+1} & \cdots & a_{nn} \end{vmatrix}
\end{aligned}$$

This equality can also be seen directly by expanding the determinant on the right according to column  $j$ .

If we denote this determinant by  $D$ , then we have proved that the unique solution of the given system is

$$x_1 = \frac{D_1}{D}, \quad x_2 = \frac{D_2}{D}, \quad \dots, \quad x_n = \frac{D_n}{D}$$

*Example* Solve by Cramer's rule

$$\begin{aligned} x - y + 2z &= 4 \\ 2x + y - z &= 3 \\ 4x - y + 4z &= 9 \end{aligned}$$

(This is example 3 of §3.)

We have

$$\begin{aligned} D &= \begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & -1 \\ 4 & -1 & 4 \end{vmatrix} = 3, \\ D_1 &= \begin{vmatrix} 4 & -1 & 2 \\ 3 & 1 & -1 \\ 9 & -1 & 4 \end{vmatrix} = 9, \\ D_2 &= \begin{vmatrix} 1 & 2 & 2 \\ 2 & 3 & -1 \\ 4 & 9 & 4 \end{vmatrix} = -15, \\ D_3 &= \begin{vmatrix} 1 & -1 & 4 \\ 2 & 1 & 3 \\ 4 & -1 & 9 \end{vmatrix} = -6 \end{aligned}$$

$$\text{Hence, } x = \frac{D_1}{D} = 3, \quad y = \frac{D_2}{D} = -5, \quad z = \frac{D_3}{D} = -2$$

### Exercises

1 Solve the following systems:

- |                        |                      |
|------------------------|----------------------|
| a) $2x + y = 3$        | d) $x - y + 2w = 0$  |
| $y + 2z = 1$           | $3y - 2z + 3w = 0$   |
| $x - 3z = 4$           | $y - 3w = 1$         |
| b) $x - y + z - 1 = 0$ | $5x + y - 2z = 0$    |
| $x + y - z + 2 = 0$    | e) $x + 2y - 3z = 1$ |
| $x - y - z - 3 = 0$    | $2x - y + w = 3$     |
| c) $3x - 4z = 0$       | $3x - 2z + w = 6$    |
| $2x - 3y + 5z = 3$     | $7y + 4z - 2w = 2$   |
| $x + 4y - 7z = 1$      |                      |

2 In three-dimensional analytic geometry, if every point  $(x, y, z)$  is assigned new coordinates  $(x', y', z')$  where  $x' = 3x - 4y + 2z$ ,  $y' = x - z$ ,  $z' = x$

+  $2y - 2z$ , what point  $(x, y, z)$  has been assigned the new coordinates  $(3, -1, 4)$ ?

3 Prove: If  $f(x) \equiv ax^2 + bx + c$  where  $a, b, c$  are integers, and if  $f(1), f(2), f(3)$  are divisible by the odd integer  $k$ , then  $a, b, c$  are divisible by  $k$ .

**5. Consistent and inconsistent systems** A system of linear equations is said to be consistent if there exists a solution. Otherwise it is called inconsistent.

Whether a system is consistent or not depends, naturally, upon the  $a_i$  and  $b_i$ . To investigate the dependence it is convenient to consider two matrices connected with the system.

The matrix formed by the coefficients of the unknowns, that is,

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

is called the matrix of the system.

The matrix obtained by adding to the matrix of the system an additional column composed of  $b_1, b_2, \cdots, b_m$ ,

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

is called the augmented matrix.

[We remark (ex 5, §9, Ch. 12) that either the two matrices have the same rank or the rank of the augmented matrix exceeds by one the rank of the matrix of the system.]

We establish:

#### THEOREM

*A system of linear equations is consistent if and only if the augmented matrix has the same rank as the matrix of the system.*

*Proof:* Suppose the system is consistent and  $(x_1, x_2, \cdots, x_n)$  is a solution. Then

$$b_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \quad (i = 1, 2, \cdots, m)$$

and the augmented matrix is

$$\left( \begin{array}{cccc|cccc} a_{11} & a_{12} & \cdots & a_{1n} & a_{11}x_1 + a_{12}x_2 + & \cdots & + a_{1n}x_n \\ a_{21} & a_{22} & \cdots & a_{2n} & a_{21}x_1 + a_{22}x_2 + & \cdots & + a_{2n}x_n \\ \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} & a_{m1}x_1 + a_{m2}x_2 + & \cdots & + a_{mn}x_n \end{array} \right)$$

Hence, the augmented matrix has the same rank as the matrix of the system (ex. 7, §9, Ch. 12).

To establish the converse, suppose the two matrices have rank  $k$ .

If  $k = 0$  then all the  $a_{ij}$  and  $b_i$  are zero (§9, Ch. 12), so that any set of values ( $x_1, x_2, \cdots, x_n$ ) is a solution. Suppose, therefore,  $k > 0$ .

In the matrix of the system some  $k$ -rowed minor is different from zero. By rearranging the rows and columns, if necessary, (which amounts to changing the order of the equations in the given system and renumbering the unknowns), we may and do suppose that the  $k$ -rowed minor formed by the elements in the first  $k$  rows and first  $k$  columns does not vanish, i.e.,

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdot & \cdot & \cdots & \cdot \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{vmatrix} \neq 0$$

(There is no loss in generality in doing this and it makes the subsequent discussion somewhat more convenient.)

Since this minor appears in the first  $k$  rows of the augmented matrix, the first  $k$  rows of the augmented matrix are linearly independent (§2).

Suppose  $k < m$ . Since the augmented matrix is of rank  $k$ , any  $k + 1$  of its rows are linearly dependent (§2). In particular, if  $i$  is any integer between  $k + 1$  and  $m$  inclusive,

$$\begin{array}{cccc|c} a_{11}, & a_{12}, & \cdots, & a_{1n}, & b_1 \\ a_{21}, & a_{22}, & \cdots, & a_{2n}, & b_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{k1}, & a_{k2}, & \cdots, & a_{kn}, & b_k \\ a_{i1}, & a_{i2}, & \cdots, & a_{in}, & b_i \end{array}$$

are linearly dependent. Hence, there exist numbers  $c_1, c_2, \cdots, c_k, c_i$ , not all zero, such that



$$c_1 a_{1j} + c_2 a_{2j} + \cdots + c_k a_{kj} + c_i a_{ij} = 0 \quad (j = 1, 2, \cdots, n) \\ c_1 b_1 + c_2 b_2 + \cdots + c_k b_k + c_i b_i = 0$$

$c_i \neq 0$ . For if  $c_i = 0$  the first  $k$  rows of the augmented matrix would be linearly dependent.

Since  $c_i \neq 0$  we obtain from the preceding equations

$$a_{ij} = d_1 a_{1j} + d_2 a_{2j} + \cdots + d_k a_{kj} \quad (j = 1, 2, \cdots, n) \\ b_i = d_1 b_1 + d_2 b_2 + \cdots + d_k b_k$$

where 
$$d_1 = -\frac{c_1}{c_i}, d_2 = -\frac{c_2}{c_i}, \cdots, d_k = -\frac{c_k}{c_i}$$

Now, if  $(x_1, x_2, \cdots, x_n)$  is any solution of the first  $k$  equations in the given system of  $m$  linear equations, and  $i$  is between  $k+1$  and  $m$  inclusive, then from the preceding,

$$\begin{aligned} a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \\ &= (d_1 a_{11} + d_2 a_{21} + \cdots + d_k a_{k1})x_1 + \\ &\quad (d_1 a_{12} + d_2 a_{22} + \cdots + d_k a_{k2})x_2 + \\ &\quad \cdots + (d_1 a_{1n} + d_2 a_{2n} + \cdots + d_k a_{kn})x_n \\ &= d_1(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n) \\ &\quad + d_2(a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n) + \\ &\quad \cdots + d_k(a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n) \\ &= d_1 b_1 + d_2 b_2 + \cdots + d_k b_k \\ &= b_i \end{aligned}$$

Thus, every solution of the first  $k$  equations satisfies all the equations.

If  $k = m$  the last statement is obviously true, since the first  $k$  equations then constitute the entire system.

Clearly, any solution of the entire system satisfies the first  $k$  equations. Combining this with the preceding result, we see that the first  $k$  equations and the entire system have exactly the same solutions.

To solve the system composed of the first  $k$  equations, first rewrite them in the form

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ik}x_k = b_i - a_{i,k+1}x_{k+1} - a_{i,k+2}x_{k+2} \\ - \cdots - a_{in}x_n \quad (i = 1, 2, \cdots, k).$$

If we assign to  $x_{k+1}, x_{k+2}, \cdots, x_n$  any values whatsoever, we have  $k$  linear equations in the  $k$  unknowns  $x_1, x_2, \cdots, x_k$  with a determinant

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdot & \cdot & \cdots & \cdot \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{vmatrix}$$

which is different from zero. By Cramer's rule (§4) there is a unique set of values for  $x_1, x_2, \dots, x_k$  such that these, together with the assigned values of  $x_{k+1}, x_{k+2}, \dots, x_n$ , form a solution of the first  $k$  equations.

Conversely, if  $(\lambda_1, \lambda_2, \dots, \lambda_n)$  is any solution of the first  $k$  equations, then, assigning the values  $\lambda_{k+1}, \lambda_{k+2}, \dots, \lambda_n$  to  $x_{k+1}, x_{k+2}, \dots, x_n$  respectively, these equations become a system of  $k$  linear equations in the  $k$  unknowns  $x_1, x_2, \dots, x_k$  having  $(\lambda_1, \lambda_2, \dots, \lambda_k)$  as its unique solution.

Thus, we have shown, all the solutions of the first  $k$  equations and, therefore, all the solutions of the given system of  $m$  equations, can be obtained by assigning arbitrary values to  $x_{k+1}, x_{k+2}, \dots, x_n$  and then solving the first  $k$  equations for  $x_1, x_2, \dots, x_k$ . (If  $k = n$  then, of course, none of the  $x$ 's can be assigned arbitrary values, since the first  $k$  equations then determine  $x_1, x_2, \dots, x_n$  uniquely.)

In all cases, a solution of the system exists, so that the given system is consistent, and the theorem is proved.

Actually we have proved:

#### THEOREM

*If the matrix of a system of linear equations in  $n$  unknowns has the same rank  $k$  as the augmented matrix, then all the solutions are obtainable by assigning arbitrary values to any  $n-k$  of the unknowns, provided (if  $k > 0$ ) the matrix of the coefficients of the remaining  $k$  unknowns has rank  $k$ , and then solving for the uniquely determined values of these other  $k$  unknowns.*

**Example 1** Solve the system

$$\begin{array}{rcl} x - y + 2z & = & 4 \\ 2x + y - z & = & 3 \\ 3x & + & z = 5 \end{array}$$

(This is example 1 of §3).

The matrix of the system

$$\begin{pmatrix} 1 & -1 & 2 \\ 2 & 1 & -2 \\ 3 & 0 & 1 \end{pmatrix}$$

has rank two, and the augmented matrix

$$\begin{pmatrix} 1 & -1 & 2 & 4 \\ 2 & 1 & -1 & 3 \\ 3 & 0 & 1 & 5 \end{pmatrix}$$

has rank three. Therefore, the system is inconsistent.

*Example 2* Solve the system

$$\begin{aligned} x - y + 2z &= 4 \\ 2x + y - z &= 3 \\ 4x - y + 3z &= 11 \end{aligned}$$

(This is example 2 of §3).

The matrix of the system

$$\begin{pmatrix} 1 & -1 & 2 \\ 2 & 1 & -1 \\ 4 & -1 & 3 \end{pmatrix}$$

and the augmented matrix

$$\begin{pmatrix} 1 & -1 & 2 & 4 \\ 2 & 1 & -1 & 3 \\ 4 & -1 & 3 & 11 \end{pmatrix}$$

both have rank two. Hence, the system is consistent and we may assign an arbitrary value to any one of the unknowns provided the matrix of the coefficients of the remaining two unknowns has a minor of order two which is not zero. For instance, we may assign  $x$  arbitrarily since

$$\begin{vmatrix} -1 & 2 \\ 1 & -1 \end{vmatrix} \neq 0$$

If we allow  $x$  to be arbitrary and solve the first two equations for  $y$  and  $z$  in terms of  $x$ , we obtain by Cramer's rule

$$y = \frac{\begin{vmatrix} 4-x & 2 \\ 3-2x & -1 \\ -1 & 2 \\ 1 & -1 \end{vmatrix}}{10-5x}, \quad z = \frac{\begin{vmatrix} -1 & 4-x \\ 1 & 3-2x \\ -1 & 2 \\ 1 & -1 \end{vmatrix}}{7-3x}$$

**Example 3** Find all values of  $k$  for which the following system is consistent:

$$\begin{aligned} x + kz - w &= 2 - k \\ 2ky + z + (2k - 1)w &= -1 \\ x + 4y + 3z + kw &= 3 - 2k \end{aligned}$$

We first consider the rank of the matrix of the system

$$\begin{pmatrix} 1 & 0 & k & -1 \\ 0 & 2k & 1 & 2k-1 \\ 1 & 4 & 3 & k \end{pmatrix}$$

The three-rowed minor formed by the first three columns is

$$\begin{vmatrix} 1 & 0 & k \\ 0 & 2k & 1 \\ 1 & 4 & 3 \end{vmatrix} = -2(k^2 - 3k + 2)$$

which vanishes only when  $k$  is 1 or 2. Hence, when  $k$  is not 1 or 2 the rank of the matrix of the system, and therefore also the rank of the augmented matrix, is three. Therefore, the system is consistent when  $k$  is different from 1 and 2.

For  $k = 1$  the matrix of the system

$$\begin{pmatrix} 1 & 0 & 1 & -1 \\ 0 & 2 & 1 & 1 \\ 1 & 4 & 3 & 1 \end{pmatrix}$$

has rank two and the augmented matrix

$$\begin{pmatrix} 1 & 0 & 1 & -1 & 1 \\ 0 & 2 & 1 & 1 & -1 \\ 1 & 4 & 3 & 1 & 1 \end{pmatrix}$$

has rank three. Hence, the system is inconsistent.

For  $k = 2$  the matrix of the system

$$\begin{pmatrix} 1 & 0 & 2 & -1 \\ 0 & 4 & 1 & 3 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

has rank two and the augmented matrix

$$\begin{pmatrix} 1 & 0 & 2 & -1 & 0 \\ 0 & 4 & 1 & 3 & -1 \\ 1 & 4 & 3 & 2 & -1 \end{pmatrix}$$

also has rank two. Hence, the system is consistent.

**6. Homogeneous systems** If all the right sides in a system of linear equations are zero, i.e., if  $b_1 = b_2 = \dots = b_m = 0$ , the system is called a system of homogeneous linear equations or, briefly, a homogeneous system. Otherwise it is called a non-homogeneous system.

Since  $x_1 = 0, x_2 = 0, \dots, x_n = 0$  is obviously a solution of a homogeneous system in  $n$  unknowns, every homogeneous system is consistent. This can also be seen from the fact that the matrix of the system and the augmented matrix necessarily have the same rank, since the latter is obtained from the former merely by adding a column of zeros.

The solution  $(0, 0, \dots, 0)$  is called the trivial solution.

If the rank of the matrix of the system is  $n$ , the number of unknowns, there can be no solution other than the trivial one. For in this case some  $n$ -rowed minor of the matrix of the system is non-zero, so that by Cramer's rule the corresponding  $n$  equations have a unique solution. This unique solution must be the trivial one, so that there is no other.

On the other hand if the rank of the matrix of the system is less than  $n$ , there are other solutions besides the trivial one. For if the rank is  $k < n$ , certain  $n - k$  of the unknowns can be assigned arbitrary non-zero values, the remaining unknowns then being uniquely determined.

We have shown, therefore:

#### THEOREM

*A homogeneous system of linear equations has a non-trivial solution if and only if the rank of the matrix of the system is less than the number of unknowns.*

#### COROLLARY

*If the number of equations in a homogeneous system equals the number of unknowns, there exists a non-trivial solution if and only if the determinant of the system is zero.*

*Proof:* This follows immediately from the theorem, since the rank of the matrix of the system is less than the number of unknowns if and only if the determinant of the system is zero.

### COROLLARY

*If there are fewer equations in a homogeneous system than the number of unknowns, there exists a non-trivial solution.*

*Proof:* The rank of the matrix of the system cannot exceed the number of equations. Therefore, the rank is less than the number of unknowns. Hence, the theorem applies.

*Example* Find all values of  $k$  for which the following system has a non-trivial solution:

$$\begin{aligned} 3x - 2ky + kz &= 0 \\ x + y - z &= 0 \\ kx - 4y + 3z &= 0 \end{aligned}$$

The number of equations equals the number of unknowns. Hence, there is a non-trivial solution if and only if the determinant of the system

$$\begin{vmatrix} 3 & -2k & k \\ 1 & 1 & -1 \\ k & -4 & 3 \end{vmatrix}$$

vanishes. This determinant equals  $k^2 + 2k - 3 = (k - 1)(k + 3)$ .

Thus, there is a non-trivial solution only when  $k$  is 1 or  $-3$ .

### Exercises

1 Solve the following systems of non-homogeneous linear equations, if consistent:

$$\begin{aligned} \text{a) } 2x - 3y + 4z &= 0 \\ x - 10z &= 3 \\ x - y - 2z &= 1 \end{aligned}$$

$$\begin{aligned} \text{b) } 3x + 2y + z &= 1 \\ 6x + 4y - z &= 2 \\ 3x + 2y - 2z &= 1 \\ 9x + 6y &= 3 \end{aligned}$$

$$\begin{aligned} \text{c) } 2x - y + z &= 3 \\ x - 3z &= 4 \\ 3x - 2y + 5z &= 1 \end{aligned}$$

$$\begin{aligned} \text{d) } 2x + 3y - 5z - 7w &= 3 \\ x - 4z - 3w &= 1 \\ 3y + 3z - w &= 2 \end{aligned}$$

$$\begin{aligned} \text{e) } 3x - y + 2z + w &= 0 \\ 2x + y + z - w &= 1 \\ 2x - 4y + 2z - w &= 4 \end{aligned}$$

$$\begin{aligned} \text{f) } x - y + 2z - 3w &= 2 \\ 3x - 2y - z + 2w &= 6 \\ 9x - 7y + 4z - 5w &= 18 \end{aligned}$$

**2** Solve the following systems of homogeneous linear equations:

a)  $x - y + 2z = 0$

$$x + 3y - 2z = 0$$

$$3y + z = 0$$

b)  $3x - 9y + 4z = 0$

$$x + y + z = 0$$

$$5x - 19y + 7z = 0$$

c)  $x + y + z + w = 0$

$$x + z + w = 0$$

$$y + w = 0$$

d)  $x + y + z - w = 0$

$$x + y - z - w = 0$$

$$x - y - z - w = 0$$

$$x - y + z - w = 0$$

e)  $2x + y + z + w = 0$

$$x + 2y + z + w = 0$$

$$x + y + 2z + w = 0$$

$$2y + 2z + w = 0$$

f)  $2x - 3y + 4z - w = 0$

$$x + y - 3z + w = 0$$

$$x - 4y + z + 2w = 0$$

$$5y - 10z + 3w = 0$$

g)  $2x - 2y + z + w = 0$

$$x + y + z - 2w = 0$$

$$3y - 2z - w = 0$$

$$3x + 2y - 2w = 0$$

**3** Determine the values of  $k$  for which the following systems are consistent, and find the solutions for these values of  $k$ :

a)  $3x - 4y + 2z = 0$

$$x + y - 2z = 0$$

$$5x - 2y - 2z = k$$

b)  $x - y + kz = 1$

$$2x + y + 3z = 0$$

$$3x + (k^2 + 1)z = 1$$

c)  $2x - 3y - z = k$

$$x + y + kz = 2k - 1$$

$$4x - y + (2k - 1)z = 3$$

d)  $x - ky + 2k = 0$

$$kx - 4y + 5 = 0$$

$$x + 2y - 1 = 0$$

e)  $x - y = k^2$

$$y - z = -3k$$

$$z - w = 0$$

$$w - x = 2$$

f)  $5x - ky + 3z + 2w = 6$

$$3x + 2y - kz + w = 4k$$

$$x - 8y + 9z + w = 0$$

g)  $x + y - z + kw = k + 1$

$$x - y + kz = k$$

$$3x + (k - 1)z + kw = 2k$$

h)  $3x + 9y - 5kz + w = 2k$

$$x + 5y - 7z + w = k$$

$$x - y + 2kz - w = k$$

**4** Find the values of  $k$  for which there is a non-trivial solution, and solve the systems for these values of  $k$ :

a)  $3x - 4y + 2z = 0$

$$4x + kz = 0$$

$$4ky - z = 0$$

b)  $kx - y + z = 0$

$$2x + y - 2kz = 0$$

$$x + 2y - 2(2k - 3)z = 0$$

c)  $x + ky = 0$

$y + kz = 0$

$z + kw = 0$

$w + kx = 0$

d)  $y + kz + (1 + k)w = 0$

$x + (1 + k)z + kw = 0$

$kx + (1 + k)y + w = 0$

$(1 + k)x + ky + z = 0$

e)  $2x - 2y + kz - kw = 0$

$2x - y + z = 0$

$y - 2z + kw = 0$

$(k + 1)x - 2y = 0$

f)  $-15x + 5y + 9kz = 0$

$x - 2y + 3z = 0$

$kx - z = 0$

$ky + 2z = 0$

5 For what values of  $x, y, z$  are  $z - 2x, 3z - 2y, 2x - y$  proportional to  $x, y, z$ ?

6 If, in three dimensional analytic geometry, to each point  $(x, y, z)$  in space we assign new coordinates  $(x', y', z')$  where  $x' = 2x - 2y + 3z, y' = 2x - 2y + 8z, z' = x - 3y + 8z$ , what points, if any, have their coordinates unchanged?

7 If the system

$$x + ky - kz = 0$$

$$(k + 1)x - 2y + 3z = 0$$

$$(ak + b + 1)x + ay = 0$$

has a non-trivial solution for every value of  $k$ , determine  $a$  and  $b$ .

8 Prove: If the determinant of a system of  $n$  linear equations in  $n$  unknowns is zero, then there exists no solution or infinitely many solutions.

9 Prove: If  $n + 1$  linear equations in  $n$  unknowns are consistent, the determinant of the augmented matrix is zero.

10 Prove: If the rank of the matrix of a homogeneous system in  $n$  unknowns is  $n - 1$ , then any two solutions are linearly dependent.

11 Prove: If  $(x_1, x_2, \dots, x_n)$  and  $(y_1, y_2, \dots, y_n)$  are solutions of a homogeneous system and  $\lambda, \mu$  are any numbers, then  $(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, \dots, \lambda x_n + \mu y_n)$  is also a solution.

12 If in the system  $a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, (i = 1, 2, \dots, m)$  we replace all the right sides by zero, we obtain what is called the associated homogeneous system. Let  $(\lambda_1, \lambda_2, \dots, \lambda_n)$  be a particular solution of the non-homogeneous system. Prove: If  $(y_1, y_2, \dots, y_n)$  is a solution of the associated homogeneous system, then  $(y_1 + \lambda_1, y_2 + \lambda_2, \dots, y_n + \lambda_n)$  is a solution of the non-homogeneous system and, conversely, every solution of the non-homogeneous system is obtain-



able in this way from some solution of the associated homogeneous system.

**7. Linear dependence of polynomials** We say the polynomials  $f(x)$  and  $g(x)$  are proportional if one of them is identically equal to the other multiplied by a constant factor. We might, if we like, broaden this concept of proportionality by permitting the factor to be any polynomial, instead of restricting it to be a constant. This would be useful for some purposes, but we shall not do so here. As in §1, however, we extend the restricted concept of proportionality to any number of polynomials.

We define the polynomials  $f_1(x), f_2(x), \dots, f_m(x)$ ,  $m \geq 1$ , to be linearly dependent if there exist constants  $c_1, c_2, \dots, c_m$ , not all zero, such that  $c_1f_1(x) + c_2f_2(x) + \dots + c_mf_m(x) \equiv 0$ .

If no such constants exist, the polynomials are said to be linearly independent.

For two polynomials linear dependence is the same as proportionality.

*Example 1* Show that  $f_1(x) \equiv x - 1$ ,  $f_2(x) \equiv 2x + 3$ ,  $f_3(x) \equiv 1$  are linearly dependent.

This is obvious since  $2f_1(x) - f_2(x) + 5f_3(x) \equiv 0$ .

Here it is a simple matter to guess the constants. We shall see below how to determine whether there is linear dependence without guessing the constants, and we show how to find the constants.

*Example 2* Show that  $f_1(x) \equiv x - 1$ ,  $f_2(x) \equiv 2x + 3$ ,  $f_3(x) \equiv x^2$  are linearly independent.

Suppose  $c_1f_1(x) + c_2f_2(x) + c_3f_3(x) \equiv 0$  where  $c_1, c_2, c_3$  are constants. Then

$$\begin{aligned} c_1(x - 1) + c_2(2x + 3) + c_3x^2 &\equiv 0 \\ c_3x^2 + (c_1 + 2c_2)x + (3c_2 - c_1) &\equiv 0 \end{aligned}$$

This requires (§4 Ch. 2)  $c_3 = 0$ ,  $c_1 + 2c_2 = 0$ ,  $3c_2 - c_1 = 0$ . Solving these equations for  $c_1, c_2, c_3$ , we find that they are all zero.

Linear dependence of polynomials is closely related to linear dependence of constants. In fact:

## THEOREM

If  $f_i(x) \equiv a_{i0}x^n + a_{i1}x^{n-1} + \cdots + a_{i,n-1}x + a_{in}$  ( $i = 1, 2, \cdots, m$ ), then  $f_1(x), f_2(x), \cdots, f_m(x)$  are linearly dependent if and only if the  $m$  sets of  $n + 1$  constants  $a_{i0}, a_{i1}, \cdots, a_{in}$  ( $i = 1, 2, \cdots, m$ ) are linearly dependent.

(The polynomials are not necessarily of the same degree since no assumption is being made concerning which, if any, of the coefficients are different from zero.)

*Proof:*

$$\begin{aligned} c_1 f_1(x) + c_2 f_2(x) + \cdots + c_m f_m(x) \\ &\equiv c_1(a_{10}x^n + a_{11}x^{n-1} + \cdots + a_{1,n-1}x + a_{1n}) \\ &\quad + c_2(a_{20}x^n + a_{21}x^{n-1} + \cdots + a_{2,n-1}x + a_{2n}) + \\ &\quad \cdots + c_m(a_{m0}x^n + a_{m1}x^{n-1} + \cdots + a_{m,n-1}x + a_{mn}) \\ &\equiv (c_1 a_{10} + c_2 a_{20} + \cdots + c_m a_{m0})x^n \\ &\quad + (c_1 a_{11} + c_2 a_{21} + \cdots + c_m a_{m1})x^{n-1} + \\ &\quad \cdots + (c_1 a_{1,n-1} + c_2 a_{2,n-1} + \cdots + c_m a_{m,n-1})x \\ &\quad + (c_1 a_{1n} + c_2 a_{2n} + \cdots + c_m a_{mn}) \end{aligned}$$

This vanishes identically if and only if

$$\begin{aligned} c_1 a_{10} + c_2 a_{20} + \cdots + c_m a_{m0} &= 0 \\ c_1 a_{11} + c_2 a_{21} + \cdots + c_m a_{m1} &= 0 \\ \cdot &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ c_1 a_{1n} + c_2 a_{2n} + \cdots + c_m a_{mn} &= 0 \end{aligned}$$

Thus, the given polynomials are linearly dependent if and only if the  $m$  sets of constants are linearly dependent (§1).

*Remark* When the polynomials are linearly dependent the multipliers  $c_1, c_2, \cdots, c_m$  can be obtained by the method of §2.

*Example* In example 1 above, we have three sets of constants, 1, -1 and 2, 3 and 0, 1, with two constants in each set. Since there are more sets than numbers in each set, we certainly have linear dependence (§2).

To find  $c_1, c_2, c_3$  we proceed (as in §2) to add a column of zeros to make the number of constants in each set equal to the number of sets. We obtain

$$\begin{array}{ccc} 1, & -1, & 0 \\ 2, & 3, & 0 \\ 0, & 1, & 0 \end{array}$$

The matrix formed by these numbers has rank two.

For  $c_1, c_2, c_3$  we may take the cofactors of the elements in the last column in the determinant of the matrix.\* We obtain  $c_1 = 2, c_2 = -1, c_3 = 5$ .

From the preceding theorem and the theorems of §2 we have:

#### COROLLARY

*The polynomials  $a_{i0}x^n + a_{i1}x^{n-1} + \dots + a_{i,n-1}x + a_{in}, (i = 1, 2, \dots, m), m \leq n + 1$ , are linearly dependent if and only if the matrix of the coefficients*

$$\begin{pmatrix} a_{10} & a_{11} & \dots & a_{1n} \\ a_{20} & a_{21} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m0} & a_{m1} & \dots & a_{mn} \end{pmatrix}$$

*has rank less than  $m$ . If  $m > n + 1$  the polynomials are necessarily linearly dependent.*

#### Exercises

- Determine whether the following sets of polynomials are linearly dependent and, if they are, find multipliers  $c_i$ :
  - $x^2 - 2x + 3, x - 1, 2$
  - $x^2 + 7x + 4, x^2 + 5x - 1, 2x + 5$
  - $x^3, x^2, x^2 - 1$
  - $x^3 + x^2 - 3x - 1, 2x^3 - x^2 - 4x + 1, x^3 - 5x^2 + x$
  - $3x^6 - 7x^4 + 4x^2 + 2x - 1, 2x^6 - 10x^5 - 10x^3 + 7x^2 - x, 4x^6 + 10x^5 - 4x^3 + x^2 + 5x - 2$
  - $x^n - nx^{n-1} - a, x^n + nx^{n-1} + a, x^{n-1} + 1$ , where  $a$  is a constant and  $n > 1$
  - $x^n - nx + 1, 2x^n - 7x + 1, x + 1$ , where  $n > 1$
- Prove: A single polynomial is linearly dependent if and only if it vanishes identically.
- Prove: If among  $f_1(x), f_2(x), \dots, f_m(x)$  there are  $n < m$  polynomials which are linearly dependent, then all  $m$  polynomials are linearly dependent.
- Prove: If  $f_1(x), f_2(x), \dots, f_m(x)$  have different degrees, they are linearly independent.
- \*5 Prove: If  $f_1(x), \dots, f_m(x)$  are linearly dependent, then  $g(x)f_1(x), \dots, g(x)f_m(x)$  are linearly dependent. Establish the converse if  $g(x) \not\equiv 0$ .
- 6 Prove: If  $f_1(x), \dots, f_m(x)$  are linearly dependent then  $f_1(g(x)), \dots, f_m(g(x))$  are linearly dependent.

- 7 Prove: If  $f_1(x), \dots, f_n(x)$  are linearly dependent, their derivatives are linearly dependent. Is the converse true?
- 8 Prove:  $f(x)$  is identically zero or of degree at most  $k$  if and only if  $f(x), f'(x), f''(x), \dots, f^{(k+1)}(x)$  are linearly dependent.
- 9 Prove:  $f_1(x), f_2(x), \dots, f_n(x)$  are linearly dependent if and only if

$$\begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_n(x) \\ f'_1(x) & f'_2(x) & \cdots & f'_n(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)}(x) & f_2^{(n-1)}(x) & \cdots & f_n^{(n-1)}(x) \end{vmatrix}$$

vanishes identically.

[This determinant is called the Wronskian of  $f_1(x), f_2(x), \dots, f_n(x)$ .]

**8. Linear equations in a field** If the elements of a determinant are required to be numbers in a given field  $\mathfrak{F}$ , instead of being allowed to be any complex numbers, the theory presented in Ch. 12 is still valid. For, in defining determinants and developing their properties, the only operations performed upon the elements are the rational operations, and the only properties of these operations which are used hold in every field. In particular, if the elements of a determinant lie in a field  $\mathfrak{F}$  then the determinant is a number in  $\mathfrak{F}$ .

It follows that the small part of the theory of matrices in §9, Ch. 12, where the elements were allowed to be any complex numbers, also applies to matrices whose elements are required to be in a given field.

The theory of linear dependence also carries over to any field. If  $a_{1i}, a_{2i}, \dots, a_{mi}$  ( $i = 1, 2, \dots, m$ ) are  $m$  sets of  $n$  numbers in  $\mathfrak{F}$ , they are said to be linearly dependent over  $\mathfrak{F}$  if there exist numbers  $c_1, c_2, \dots, c_m$  in  $\mathfrak{F}$  and not all zero such that  $c_1 a_{1j} + c_2 a_{2j} + \dots + c_m a_{mj} = 0$  for  $j = 1, 2, \dots, n$ .

It follows as before that if  $m \leq n$  the  $m$  sets of constants in  $\mathfrak{F}$  are linearly dependent over  $\mathfrak{F}$  if and only if the rank of their matrix is less than  $m$ . If  $m > n$  the  $m$  sets are always linearly dependent over  $\mathfrak{F}$ .

Since the theory of linear equations depends only upon the theories of determinants, matrices and linear dependence, and only the rational operations are used in the development of the theory, it follows that if the  $a_{ij}$  and  $b_i$  in the system of equations  $a_{11}x_1 +$

$a_{i2}x_2 + \cdots + a_{in}x_n = b_i$  ( $i = 1, 2, \cdots, m$ ) belong to a field  $\mathfrak{F}$  and the numbers  $x_1, x_2, \cdots, x_n$  in a solution  $(x_1, x_2, \cdots, x_n)$  are required to be in  $\mathfrak{F}$ , then the entire discussion of linear equations in this chapter applies.

We might also remark that all the preceding theory concerning determinants, matrices, linear dependence, and linear equations is independent of any particular field in which the elements lie. In particular:

(a) If the elements of a determinant lie in  $\mathfrak{F}$  and also in  $\mathfrak{F}'$ , then the determinant also lies in both fields. Thus, the value of a determinant does not depend upon any particular field in which the elements lie.

(b) If the elements of a matrix lie in  $\mathfrak{F}$ , the rank of the matrix does not depend upon  $\mathfrak{F}$ . Since the rank is determined by the values of the minors of the matrix, and these values do not depend upon  $\mathfrak{F}$ , the rank is the same whether we regard the elements as belonging to the field  $\mathfrak{F}$  or to any other field which contains them.

(c) If  $m$  sets of constants are linearly dependent over  $\mathfrak{F}$ , they are linearly dependent over any field  $\mathfrak{F}'$  which contains these constants. For, if they are linearly dependent over  $\mathfrak{F}$ , the multipliers  $c_1, c_2, \cdots, c_m$  can be determined as the values, or the negatives of the values, of certain minors of the matrix. Hence, the multipliers belong to  $\mathfrak{F}$  and also to  $\mathfrak{F}'$ .

(d) If the  $a_{ij}$  and  $b_i$  in a system of  $m$  linear equations in  $n$  unknowns lie in  $\mathfrak{F}$ , and  $\mathfrak{F}'$  is any other field containing these numbers, then the system is consistent over  $\mathfrak{F}$ , that is, there is a solution  $(x_1, x_2, \cdots, x_n)$  where  $x_1, x_2, \cdots, x_n$  are in  $\mathfrak{F}$ , if and only if it is consistent over  $\mathfrak{F}'$ . This follows from the fact that the ranks of the matrix of the system and the augmented matrix do not depend upon the field containing the elements. We remark, however, that it is possible for the system to have a solution  $(x_1, x_2, \cdots, x_n)$  in which  $x_1, x_2, \cdots, x_n$  lie in  $\mathfrak{F}$  but not in  $\mathfrak{F}'$ . For, if some of the unknowns can be assigned arbitrary values, the remaining unknowns then being uniquely determined, it is possible to choose the assigned values in such a way that they lie in  $\mathfrak{F}$  but not in  $\mathfrak{F}'$ .

## ELIMINATION

**1. Definition of elimination** It is sometimes necessary to determine whether polynomials  $f(x)$  and  $g(x)$  have a common root when it is impossible or inconvenient in any practical way to obtain all the roots of either one. Obviously, they can have a common root only if some relation exists among their coefficients. The determination of a condition on the coefficients which is satisfied if and only if the polynomials have a common root is called eliminating  $x$  from the equations  $f(x) = 0$ ,  $g(x) = 0$ .

*Example 1* Eliminate  $x$  from  $x^3 + 2x^2 + (a - 1)x + a = 0$  and  $x^2 + x + a - 3 = 0$ .

Multiplying both sides of the second equation by  $x$  and subtracting from the corresponding sides of the first, we have  $x^2 + 2x + a = 0$ . Multiplying both sides of this equation by  $x$  and subtracting from the first of the given equations, we have  $-x + a = 0$ .

Thus,  $x = a$  is the only possible common root.

Letting  $x = a$  in the second of the given equations, we have  $a^2 + 2a - 3 = 0$ , so that  $a$  is 1 or  $-3$ .

For  $a = -3$  the given equations are  $x^3 + 2x^2 - 4x - 3 = 0$  and  $x^2 + x - 6 = 0$ , with  $x = a = -3$  as a common root.

For  $a = 1$  the given equations are  $x^3 + 2x^2 + 1 = 0$  and  $x^2 + x - 2 = 0$ , which have no common root (since the only possible common root  $x = a = 1$  is not a root of the first).

Thus, the equations have a common root if and only if  $a = -3$ .

When we assumed that  $x$  has the same value in both equations and arrived at the conclusion that  $a$  is 1 or  $-3$ , we showed: if there is a common root then  $a$  is 1 or  $-3$ . The converse is not true since it is possible for  $a$  to have one of the values 1 or  $-3$  without the given equations having a common root. Thus, the original elimination was faulty, but direct testing of the condition obtained supplied the necessary correction.

*Example 2* Eliminate  $x$  from  $x^2 + ax + b = 0$  and  $x^2 + cx + d = 0$ .

We can solve one of the equations and substitute the roots into the other. Actually, however, we do not need the roots. For, if  $r_1, r_2$  are the roots of the first, then there is a common root if and only if  $(r_1^2 + cr_1 + d)(r_2^2 + cr_2 + d) = 0$ .

Multiplying the two factors, we obtain the condition

$$r_1^2 r_2^2 + cr_1 r_2 (r_1 + r_2) + d(r_1^2 + r_2^2) + c^2 r_1 r_2 + cd(r_1 + r_2) + d^2 = 0$$

But

$$r_1 r_2 = b, r_1 + r_2 = -a, r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2r_1 r_2 = a^2 - 2b$$

Thus, the condition is

$$b^2 - abc + (a^2 - 2b)d + bc^2 - acd + d^2 = 0.$$

In theory, this is a perfectly general method of elimination applicable to polynomials of all degrees, but it is difficult in practice except when the degrees of the polynomials are small.

**2. Resultants** If two polynomials have a common root  $r$ , they have a common factor  $x - r$ . Conversely, if they have a common factor which is not a constant, they have a common root. Thus, the condition for the existence of a common root is the condition for the existence of a non-constant common factor.

The condition for the existence of a non-constant common factor is the vanishing of the last remainder (the one which does not involve  $x$ ) in the Euclidean algorithm (§8, Ch. 2).

For example, if  $f(x) \equiv (a-1)x^2 + x + (a-1)^2$ ,  $g(x) \equiv ax^2 + x + (a-1)a$ , the Euclidean algorithm is

$$\begin{aligned} f(x) &\equiv \frac{a-1}{a} g(x) + \frac{x}{a} \\ g(x) &\equiv (a^2x + a) \frac{x}{a} + a(a-1) \end{aligned}$$

Since the last remainder is  $a(a-1)$ , apparently we may say that  $f(x)$  and  $g(x)$  have a common root if and only if  $a$  is 0 or 1. Actually, the algorithm gives us no such right, since for  $a = 0$

certain parts of the algorithm fail to exist. However, we do have the right to say that if  $a$  is not 0 or 1 there is no common root, and if  $a = 1$  there is.

For  $a = 0$  the algorithm does not apply, but in this case  $f(x) = -x^2 + x + 1$  and  $g(x) \equiv x$ , and we see there is no common root.

It often happens, as in this example, that the use of the Euclidean algorithm leads to the inconvenience of requiring special consideration for some values of the coefficients. The trouble arises from the fact that in the quotients and remainders some of the coefficients may not be polynomials in the coefficients of  $f(x)$  and  $g(x)$ .

A polynomial in the coefficients of  $f(x)$  and  $g(x)$  which vanishes if and only if  $f(x)$  and  $g(x)$  have a common root is called a resultant or eliminant of  $f(x)$  and  $g(x)$ . The Euclidean algorithm does not always lead to a resultant. Sylvester's method of elimination, which we shall present, does, and also has the advantage of greater simplicity.

### Exercises

Eliminate  $x$  from the following pairs of equations and, if possible, find the common roots:

a)  $ax^2 + 2x + a = 0$

$$a^2x^2 + ax + a^2 - 1 = 0$$

b)  $ax^2 + 2x + a = 0$

$$a^2x^2 + a^2x - 4x + a^2 = 0$$

c)  $x^3 - 3x + 2 = 0$

$$x^2 + ax^2 - 1 = 0$$

d)  $x^3 + bx^2 + x + a = 0$

$$x^2 + (b-a)x + 1 - ab = 0$$

e)  $x^3 - 3x + 2 = 0$

$$x^2 + ax + b = 0$$

f)  $x^3 + ax^2 + bx + c = 0$

$$x^2 + dx + e = 0$$

g)  $x^3 + ax^2 + a + 1 = 0$

$$x^3 - x + 2a + 2 = 0$$

### 3. Linear dependence and common factors Let

$$f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \quad n \geq 1$$

$$g(x) \equiv b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m, \quad m \geq 1$$

We may or may not have  $m = n$ . We are not at the moment making any hypothesis concerning which, if any, of the  $a$ 's and  $b$ 's are different from zero.

Let  $1 \leq k \leq p$ , where  $k$  and  $p$  are integers and  $p$  does not exceed either  $m$  or  $n$ .



## THEOREM

If  $f(x)$  and  $g(x)$  have a common factor of degree  $p$ , then any  $m + n - k - p + 2$  of the polynomials  $x^i f(x)$  ( $i = 0, 1, \dots, m - k$ ),  $x^j g(x)$  ( $j = 0, 1, \dots, n - k$ ) are linearly dependent.

(For a discussion of linear dependence of polynomials see §7, Ch. 13.)

*Proof:* Suppose

$$\begin{aligned} f(x) &\equiv \varphi(x)F(x) \\ g(x) &\equiv \varphi(x)G(x) \end{aligned}$$

where  $\varphi(x)$  is of degree  $p$  and  $F(x)$  and  $G(x)$  are identically zero or of degrees  $n - p$  and  $m - p$  at most. Then

$$\begin{aligned} x^i f(x) &\equiv x^i \varphi(x) F(x) \equiv \varphi(x) F_i(x) \quad \text{where } F_i(x) \equiv x^i F(x); \\ x^j g(x) &\equiv x^j \varphi(x) G(x) \equiv \varphi(x) G_j(x) \quad \text{where } G_j(x) \equiv x^j G(x). \end{aligned}$$

Since  $i = 0, 1, \dots, m - k$ , the maximum possible degree of  $F_i(x)$  is  $m + n - k - p$ .

Since  $j = 0, 1, \dots, n - k$ , the maximum possible degree of  $G_j(x)$  is also  $m + n - k - p$ . By the corollary in §7, Ch. 13, any  $m + n - k - p + 2$  of the  $F_i(x)$  and  $G_j(x)$  are linearly dependent. Therefore (ex. 5, §7, Ch. 13), any  $m + n - k - p + 2$  of the polynomials  $x^i f(x)$  and  $x^j g(x)$  are linearly dependent, which establishes the theorem.

## THEOREM

If  $a_0$  or  $b_0$  is different from zero and any  $m + n - k - p + 2$  of the polynomials  $x^i f(x)$  ( $i = 0, 1, \dots, m - k$ ),  $x^j g(x)$  ( $j = 0, 1, \dots, n - k$ ) are linearly dependent, then  $f(x)$  and  $g(x)$  have a common factor of degree  $p$  or higher.

*Proof:* Suppose, to be specific, that  $a_0 \neq 0$ .

By hypothesis,  $x^i f(x)$  ( $i = 0, 1, \dots, m - k$ ) and  $x^j g(x)$  ( $j = 0, 1, \dots, n - p$ ) are linearly dependent. Therefore, there exist constants  $\lambda_0, \lambda_1, \dots, \lambda_{m-1}, \mu_0, \mu_1, \dots, \mu_{n-p}$ , not all zero, such that

$$\lambda_0 f(x) + \lambda_1 x f(x) + \dots + \lambda_{m-1} x^{m-1} f(x) + \mu_0 g(x) + \mu_1 x g(x) + \dots + \mu_{n-p} x^{n-p} g(x) \equiv 0.$$

Hence,  
where

$$\begin{aligned} A(x) f(x) + B(x) g(x) &\equiv 0 \\ A(x) &\equiv \lambda_0 + \lambda_1 x + \dots + \lambda_{m-1} x^{m-1} \\ B(x) &\equiv \mu_0 + \mu_1 x + \dots + \mu_{n-p} x^{n-p} \end{aligned}$$

If  $B(x) \equiv 0$  then  $A(x)f(x) \equiv 0$ . Since  $f(x) \not\equiv 0$ , this requires  $A(x) \equiv 0$ . But  $A(x) \equiv 0$  and  $B(x) \equiv 0$  is impossible since not all the  $\lambda$ 's and  $\mu$ 's are zero. Therefore,  $B(x) \not\equiv 0$ . Hence,  $B(x)$  is of degree  $n - p$  or less.

It follows (ex. 10, §10, Ch. 2) that  $f(x)$  and  $g(x)$  have a common factor whose degree is at least  $p$ .

**4. Condition for common roots** In considering the number of common roots of  $f(x)$  and  $g(x)$  we agree to count each root as often as its multiplicity. Thus, the statement that  $f(x)$  and  $g(x)$  have  $p$  common roots means that they have a common factor of degree  $p$ .

In view of the theorems of §3, to obtain a convenient condition for the existence of  $p$  common roots we have only to express conveniently the condition that any  $m + n - k - p + 2$  of the polynomials  $x^i f(x)$  ( $i = 0, 1, \dots, m - k$ ) and  $x^j g(x)$  ( $j = 0, 1, \dots, n - k$ ) are linearly dependent. This can be done by means of the matrix of the coefficients of these polynomials.

We have

$$\begin{aligned}
x^{m-k}f(x) &= a_0x^{m+n-k} + a_1x^{m+n-k-1} + \dots + a_{n-1}x^{m-k+1} + a_nx^{m-k} \\
x^{m-k-1}f(x) &= a_0x^{m+n-k-1} + \dots + a_{n-2}x^{m-k+1} + a_{n-1}x^{m-k} + a_nx^{m-k-1} \\
. & . . . . . \\
x^f(x) &= a_1x^{n+1} + a_1x^n + . . . + a_{n-1}x^2 + a_nx \\
f(x) &= a_0x^n + . . . + a_{n-2}x^2 + a_{n-1}x + a_n \\
x^{n-k}g(x) &= b_0x^{m+n-k} + b_1x^{m+n-k-1} + . . . + b_{m-1}x^{n-k+1} + h_nx^{n-k} \\
x^{n-k-1}g(x) &= b_0x^{m+n-k-1} + . . . + b_{m-2}x^{n-k+1} + b_{m-1}x^{n-k} + b_{m,2}x^{n-k-1} \\
. & . . . . . \\
xg(x) &= b_0x^{m+1} + b_1x^m + . . . + b_{m-1}x^2 + b_mx . \\
g(x) &= b_{0,m} + . . . + b_{m-2}x^2 + b_{m-1}x + b_m
\end{aligned}$$



Since  $p \geq k$ ,  $k + p - 2 \geq 2k - 2$ . Hence  $m + n - (k + p - 2) \leq m + n - (2k - 2)$ ; that is,  $m + n - k - p + 2$  is equal to or less than the number of rows in  $\Delta_k$ . Therefore, any  $m + n - k - p + 2$  of the polynomials  $x'f(x)$ ,  $x'g(x)$  are linearly dependent if and only if any  $m + n - k - p + 2$  rows of  $\Delta_k$  are linearly dependent (§7. corollary, Ch. 13). It follows that any  $m + n - k - p + 2$  of the  $x'f(x)$ ,  $x'g(x)$  are linearly dependent if and only if the rank of  $\Delta_k$  does not exceed  $m + n - k - p + 1$ .

From the theorems of §3 we now have:

#### THEOREM

*If  $f(x)$  and  $g(x)$  have  $p$  or more common roots, then the rank of  $\Delta_k$  does not exceed  $m + n - k - p + 1$ .*

#### THEOREM

*If  $a_0$  or  $b_0$  is different from zero and the rank of  $\Delta_k$  does not exceed  $m + n - k - p + 1$ , then  $f(x)$  and  $g(x)$  have  $p$  or more common roots.*

By taking  $k = 1$  we obtain the corollaries:

#### COROLLARY 1

*If  $f(x)$  and  $g(x)$  have  $p$  or more common roots then the rank of  $\Delta_1$  does not exceed  $m + n - p$ .*

#### COROLLARY 2

*If  $a_0$  or  $b_0$  is different from zero and the rank of  $\Delta_1$  does not exceed  $m + n - p$ , then  $f(x)$  and  $g(x)$  have at least  $p$  common roots.*

By taking  $k = p$  in the theorems (in which case  $\Delta_p$  has  $m + n - 2p + 2$  rows and  $m + n - p + 1$  columns), we have the additional corollaries:

#### COROLLARY 3

*If  $f(x)$  and  $g(x)$  have  $p$  or more common roots, then the rank of  $\Delta_p$  does not exceed  $m + n - 2p + 1$ .*

#### COROLLARY 4

*If  $a_0$  or  $b_0$  is different from zero and the rank of  $\Delta_p$  does not exceed  $m + n - 2p + 1$ , then  $f(x)$  and  $g(x)$  have at least  $p$  common roots.*

$\Delta_1$  is an  $(m + n)$ -rowed square matrix. Hence, its rank does not exceed  $m + n - 1$  if and only if the determinant of  $\Delta_1$  is zero. Thus, this determinant is a polynomial in the coefficients of  $f(x)$  and  $g(x)$  which, if  $a_0$  or  $b_0$  is non-zero, vanishes if and only if  $f(x)$  and  $g(x)$  have a common root.

We denote this determinant by  $\Delta$  and call it the Sylvester resultant of  $f(x)$  and  $g(x)$ .

$\Delta_1$  is made up of two groups of rows, the first  $m$  rows formed from the coefficients of  $f(x)$  and the last  $n$  from the coefficients of  $g(x)$ . If we delete the first column of  $\Delta_1$  and also the first row of each group, we obtain  $\Delta_2$ . If we delete the first two columns of  $\Delta_1$  and also the first two rows of each group, we obtain  $\Delta_3$ .

In general,  $\Delta_p$  is obtainable from  $\Delta_1$  by deleting the first  $p - 1$  columns of  $\Delta_1$  and the first  $p - 1$  rows of each of the two groups of rows in  $\Delta_1$ .

*Example 1* Determine the number of common roots of  $f'(x) \equiv 2x^3 - x^2 - 1$  and  $g(x) \equiv 2x^3 + 3x^2 + 2x + 1$ .

We have  $m = n = 3$  and

$$\begin{aligned} x^2 f(x) &\equiv 2x^5 - x^4 - x^2 \\ xf(x) &\equiv 2x^4 - x^3 - x \\ f(x) &\equiv 2x^3 - x^2 - 1 \\ x^2 g(x) &\equiv 2x^5 + 3x^4 + 2x^3 + x^2 \\ xg(x) &\equiv 2x^4 + 3x^3 + 2x^2 + x \\ g(x) &\equiv 2x^3 + 3x^2 + 2x + 1 \end{aligned}$$

$$\Delta_1 = \begin{pmatrix} 2 & -1 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & -1 & 0 \\ 0 & 0 & 2 & -1 & 0 & -1 \\ 2 & 3 & 2 & 1 & 0 & 0 \\ 0 & 2 & 3 & 2 & 1 & 0 \\ 0 & 0 & 2 & 3 & 2 & 1 \end{pmatrix}$$

$$\Delta_2 = \begin{pmatrix} 2 & -1 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 & -1 \\ 2 & 3 & 2 & 1 & 0 \\ 0 & 2 & 3 & 2 & 1 \end{pmatrix},$$

$$\Delta_3 = \begin{pmatrix} 2 & -1 & 0 & -1 \\ 2 & 3 & 2 & 1 \end{pmatrix}$$

The determinant of  $\Delta_1$  is zero. Hence, there is at least one common root.

The rank of  $\Delta_3$  is obviously two. Hence, there cannot be three common roots (corollary 3).

Thus, if the rank of  $\Delta_2$  is four there is one common root, and if its rank is less than four there are two common roots.

$\Delta_2$  has five four-rowed minors and each of them is zero.

Therefore,  $f(x)$  and  $g(x)$  have two common roots.

**Example 2** Find the values of  $a$  for which  $x^3 - 3x + a$  and  $x^2 - ax + 1$  have a common root.

Since the leading coefficients are different from zero, there is a common root if and only if the Sylvester resultant vanishes. We have

$$\Delta = \begin{vmatrix} 1 & 0 & -3 & a & 0 \\ 0 & 1 & 0 & -3 & a \\ 1 & -a & 1 & 0 & 0 \\ 0 & 1 & -a & 1 & 0 \\ 0 & 0 & 1 & -a & 1 \end{vmatrix} = (a^2 - 4)^2$$

Thus, the polynomials have a common root if and only if  $a$  is 2 or -2.

For  $a = 2$  the polynomials are  $x^3 - 3x + 2$  and  $x^2 - 2x + 1$ , with 1 as a common root.

For  $a = -2$  the polynomials are  $x^3 - 3x - 2$  and  $x^2 + 2x + 1$ , with -1 as a common root.

### Exercises

1 Determine the number of common roots:

a)  $x^3 - 3x + 2 = 0$

$4x^3 + 9x^2 - 4 = 0$

b)  $x^3 + 3x^2 - 5x + 1 = 0$

$x^3 - 5x^2 + 3x + 1 = 0$

c)  $x^3 + 5x + 2 = 0$

$x^3 + 3x + 1 = 0$

d)  $2x^3 + x^2 - 2x - 1 = 0$

$2x^3 - x^2 - 2x + 1 = 0$

e)  $x^3 + 3x - 1 = 0$

$x^3 + 2x^2 + 1 = 0$

f)  $x^4 + 3x^2 + 2x + 3 = 0$

$x^4 + x^2 + 1 = 0$

g)  $x^3 + x + 1 = 0$

$x^4 - x^3 + x^2 - 1 = 0$

h)  $x^4 - x^3 + 2x^2 - x + 1 = 0$

$x^3 - 2x^2 + x - 2 = 0$

i)  $x^3 + 3x + 1 = 0$

$x^3 + x^2 + 3 = 0$

j)  $x^3 + x^2 + 1 + i = 0$

$x^3 + 2x - i = 0$

k)  $4x^3 + 3x^2 + 125 = 0$

$3x^3 - 4x^2 + 25 = 0$

2 Determine the number of common roots for all values of  $a$ , or of  $a$  and  $b$ :

- |   |   |
|---|---|
| a) $x - a = 0$<br>$x^3 - 3a^2x + a = 0$                         | j) $2x^3 - x^2 + a = 0$<br>$2x^3 + x^2 + x - 1 = 0$           |
| b) $x^2 + ax + a = 0$<br>$x^3 + ax + a = 0$                     | k) $x^3 + ax^2 + b = 0$<br>$x^3 + ax + b = 0$                 |
| c) $x^2 + ax + a = 0$<br>$x^3 + ax^2 + a = 0$                   | l) $x^4 + ax + a + 2 = 0$<br>$x^4 + (a + 2)x + a = 0$         |
| d) $x^2 - ax + a - 1 = 0$<br>$x^3 + x^2 - (a^2 + 1)x + a^2 = 0$ | m) $ax^4 - x^3 - 3x^2 - 5x - 2 = 0$<br>$x^2 + x + 1 = 0$      |
| e) $x^3 + 2x - 1 = 0$<br>$x^3 + ax - 1 = 0$                     | n) $x^4 - x^3 + ax^2 - x + 1 = 0$<br>$x^3 - 2x^2 + x - a = 0$ |
| f) $x^3 + ax^2 - 2x + 1 = 0$<br>$x^3 - 2x^2 + ax + 1 = 0$       | o) $x^3 + 2ax + a = 0$<br>$x^3 + 2ax + a = 0$                 |
| g) $ax^2 + bx + a = 0$<br>$x^3 - 2x^2 + 2x - 1 = 0$             | p) $x^3 + ax + b + 1 = 0$<br>$x^3 - 1 = 0$                    |
| h) $x^3 + ax + b = 0$<br>$x^2 + ax + b = 0$                     | q) $x^4 + ax^3 + 1 = 0$<br>$x^4 + bx^3 + 1 = 0$               |
| i) $x^2 - x + 1 = 0$<br>$x^4 + (a - 1)x^3 + x^2 + a = 0$        | $x^3 + ax^2 + 1 = 0$  |

3 Determine the values of  $a$  for which the following have multiple roots (see §2, Ch. 4):

- |                         |                            |
|-------------------------|----------------------------|
| a) $x^3 + 3ax + a = 0$  | c) $x^4 + 4ax^3 + 27a = 0$ |
| b) $x^4 - 4ax + 3a = 0$ |                            |

4 If  $f(x) = a(x - r)$ ,  $g(r) = b_0x^m + b_1x^{m-1} + \dots + b_m$ , show that the Sylvester resultant of  $f(x)$  and  $g(x)$  is  $a^m g(r)$ .

5 Let  $f(x)$  be of degree  $n > 0$ . By the division algorithm (§6, Ch. 2) let  $x^i g(x) = Q_i(x)f(x) + a_{i0}x^{n-1} + a_{i1}x^{n-2} + \dots + a_{i,n-1}x + a_{i,n-1}$  ( $i = 0, 1, \dots, n-1$ ). Prove  $f(x)$  and  $g(x)$  have a common root if and only if

$$\begin{vmatrix} a_{00} & \dots & a_{0,n-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,0} & \dots & a_{n-1,n-1} \end{vmatrix} = 0$$

(This method of elimination is due to Laurent.)

6 Show that there exist polynomials  $A(x)$  and  $B(x)$  such that the Sylvester resultant of  $f(x)$  and  $g(x)$  equals  $A(x)f(x) + B(x)g(x)$ . (Hint: Multiply the first column by  $x$  and add to the second. Multiply new second column by  $x$  and add to the third. Etc. Expand according to last column.)



**5. Two equations in two unknowns** Suppose we have a system of two equations  $f(x, y) = 0$ ,  $g(x, y) = 0$ , where  $f(x, y)$  and  $g(x, y)$  are polynomials in  $x$  and  $y$ , neither identically zero, and we seek all pairs of values  $(x, y)$  satisfying both equations. Such a pair of values is called a solution of the system.

We suppose that both  $x$  and  $y$  appear in the system, i.e., at least one of the polynomials has a positive degree in  $x$  and at least one a positive degree in  $y$ .

Let the polynomials, arranged according to powers of  $x$ , be

$$\begin{aligned} f(x, y) &\equiv a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y), \\ g(x, y) &\equiv b_0(y)x^m + b_1(y)x^{m-1} + \cdots + b_{m-1}(y)x + b_m(y), \end{aligned}$$

$a_0(y) \neq 0$   
 $b_0(y) \neq 0$

where the  $a_i(y)$  and  $b_i(y)$  are polynomials in  $y$ .

We may have  $n = 0$  or  $m = 0$ , but not both.

If neither  $n$  nor  $m$  is zero, we can eliminate  $x$  and obtain the Sylvester resultant, which will be a polynomial in  $y$ . We denote this resultant by  $R(y)$  and we call  $R(y) = 0$  the final equation in  $y$ .

If  $(x_0, y_0)$  is a solution of the given system, then  $f(x, y_0)$  and  $g(x, y_0)$  are polynomials in  $x$  with  $x = x_0$  as a common root. The resultant of these two polynomials in  $x$  is  $R(y_0)$ . Hence (§4),  $R(y_0) = 0$ .

If one of  $n$  and  $m$  is zero, and  $(x_0, y_0)$  is a solution, then obviously  $y_0$  is a root of that equation  $f(x, y) = 0$  and  $g(x, y) = 0$  which does not involve  $x$ . In this case we call the equation which does not involve  $x$  the final equation in  $y$ .

Thus, in all cases:

#### THEOREM

*If  $(x_0, y_0)$  is a solution of the system  $f(x, y) = 0$ ,  $g(x, y) = 0$ , then  $y_0$  is a root of the final equation in  $y$ .*

We can, in a similar way, define the final equation in  $x$  and show that  $x_0$  must be a root of that equation.

The converse of the theorem is not true. It is possible for  $y_0$  to be a root of the final equation in  $y$  without any value  $x_0$  existing such that  $(x_0, y_0)$  is a solution of the system (see example 1 below). However, this cannot happen if  $a_0(y_0) \neq 0$  or  $b_0(y_0) \neq 0$  (corollary 2, §4).

To find all the solutions of  $f(x, y) = 0$ ,  $g(x, y) = 0$ , we have only to find all the roots of  $R(y) = 0$  and then, for each such root  $y$ , find the common roots of the equations in  $x$ ,  $f(x, y) = 0$ ,  $g(x, y) = 0$ . (Or, it may be more convenient to proceed by first finding the roots of the final equation in  $x$ .)

*Example 1* Solve the system of equations  $x^2y + 2x + 1 = 0$ ,  $xy + y + 6 = 0$ .

Eliminating  $x$  by Sylvester's method, we have

$$R(y) = \begin{vmatrix} y & 2 & 1 \\ y & y+6 & 0 \\ 0 & y & y+6 \end{vmatrix} = y(y+3)(y+8)$$

The roots of the final equation in  $y$  are 0, -3, -8.

For  $y = 0$  the given equations are  $2x + 1 = 0$ ,  $6 = 0$ , with no common root.

For  $y = -3$  the given equations are  $-3x^2 + 2x + 1 = 0$ ,  $-3x + 3 = 0$ , with  $x = 1$  as a common root.

For  $y = -8$  the given equations are  $-8x^2 + 2x + 1 = 0$ ,  $-8x - 2 = 0$ , with  $x = -\frac{1}{4}$  as a common root.

Thus, the solutions of the system are  $(1, -3)$  and  $(-\frac{1}{4}, -8)$ .

*Example 2* Solve the system of equations  $y^2 - x^2 + 2y - 2x = 0$ ,  $2xy - x^2 - y^2 + 2y - 2x = 0$ .

Eliminating  $x$  by Sylvester's method, we have

$$R(y) = \begin{vmatrix} -1 & -2 & y^2 + 2y & 0 \\ 0 & -1 & -2 & y^2 + 2y \\ -1 & 2y - 2 & 2y - y^2 & 0 \\ 0 & -1 & 2y - 2 & 2y - y^2 \end{vmatrix} = 0$$

We also have

$$\Delta_2 = \begin{vmatrix} -1 & -2 & y^2 + 2y \\ -1 & 2y - 2 & 2y - y^2 \end{vmatrix}$$

Investigation of the three two-rowed minors of  $\Delta_2$  shows that the rank of  $\Delta_2$  is two except when  $y = 0$  in which case it is one.

Thus, for  $y \neq 0$  there is exactly one solution  $(x, y)$  and for  $y = 0$  there may be two. (We say "may" since the two solutions may turn out to be the same.)

For  $y = 0$  the equations are  $x^2 + 2x = 0$ ,  $x^2 + 2x = 0$ , with 0 and -2 as common roots.

For  $y \neq 0$  the common root is  $x = y$  (by the method of §6, Ch. 3).

Thus, the solutions are  $(y, y)$  for all values of  $y$ , including  $y = 0$ , and  $(-2, 0)$ .

### Exercises

Solve the following systems of equations:

- |  |   |
|--|---|
| a) $(x - y)^2 + 4 = x + 2y$<br>$xy + 2 = 2x + y$                 | b) $x^2y + x^2 - y - 1 = 0$<br>$x^2y - 2xy - x + y + 1 = 0$     |
| c) $x^2 + xy + 3y^2 = 5$<br>$x^2 + 3xy + y^2 = 5$                | d) $(x + y)(1 + xy) + xy = 0$<br>$xy(1 + x + y) + 2(x + y) = 0$ |
| e) $x^3 + xy^2 - 2x^2y - 2y = 0$<br>$xy - x^2 = 1$               | f) $x(y + a) + 4a = 0$<br>$y(x + 1) + a = 0$                    |
| f) $xy + x + y = 1$<br>$x^2y + x^2 - x - xy^2 - y^2 + y - 1 = 0$ | g) $x^2 + xy + a^2 = 0$<br>$xy + y^2 - 5a^2 = 0$                |
| g) $x^2 + xy - y = 0$<br>$x^2 + 4x - y^2 - y - 0 = 0$            | h) $xy + ax + 2 = 0$<br>$(a + b)xy + y + b = 0$                 |
| h) $xy^2 - xy - y^2 + 1 = 0$<br>$xy - y - 1 = 0$                 | i) $xy + x^2 = ay$<br>$xy + y^2 = ax$                           |
| i) $x^3 - x - y^2 + y = 0$<br>$x^2 + y^2 = 1$                    |   |

**6. Common factors of polynomials in two variables** The theory of elimination provides a way of determining whether polynomials  $f(x, y)$  and  $g(x, y)$  have a common polynomial factor.

### THEOREM

*If  $f(x, y)$  and  $g(x, y)$  are non-constant polynomials, at least one of positive degree in  $x$  and at least one of positive degree in  $y$ , then they have a common polynomial factor of positive degree in  $x$  if and only if  $R(y) \equiv 0$ .*

*Proof:* Suppose  $f(x, y)$  and  $g(x, y)$  have the common polynomial factor  $h(x, y) \equiv c_0(y)x^p + \cdots + c_p(y)$ ,  $p \geq 1$ ,  $c_0(y) \neq 0$ . If  $y_0$  is any number such that  $c_0(y_0) \neq 0$ , then  $h(x, y_0) = 0$  has at least one root  $x_0$ . Thus, for every such  $y_0$  there is a solution  $(x_0, y_0)$  of the system  $f(x, y) = 0$ ,  $g(x, y) = 0$ . Hence, every such  $y_0$  is a root of  $R(y) = 0$ . Since there are infinitely many such values of  $y_0$ ,  $R(y) \equiv 0$  (§4, Ch. 2).

Conversely, suppose  $R(y) \equiv 0$ . If

$$\begin{aligned} f(x, y) &\equiv a_0(y)x^n + \cdots + a_{n-1}(y)x + a_n(y), & a_0(y) &\neq 0 \\ g(x, y) &\equiv b_0(y)x^m + \cdots + b_{m-1}(y)x + b_m(y), & b_0(y) &\neq 0, \end{aligned}$$

then necessarily  $n \geq 1$  and  $m \geq 1$ . For, for instance, if  $n = 0$  then  $R(y) \equiv a_0(y) \neq 0$ .

If we treat  $f(x, y)$  and  $g(x, y)$  as polynomials in  $x$  and obtain a highest common factor by the Euclidean algorithm, starting the algorithm by dividing  $f$  by  $g$ , then it is easily verified (by proceeding step by step down the algorithm) that all the quotients and remainders are polynomials in  $x$  whose coefficients are quotients of polynomials in  $y$  by powers of  $b_0(y)$ . In particular, this is true of the highest common factor  $D(x, y)$  which is obtained.

If we divide  $f(x, y)$  and  $g(x, y)$  by  $D(x, y)$ , regarding these as polynomials in  $x$ , we obtain

$$f(x, y) = F(x, y)D(x, y), \quad g(x, y) = G(x, y)D(x, y)$$

where  $F, G, D$  are polynomials in  $x$  whose coefficients are quotients of polynomials in  $y$ . These equalities hold for all values of  $x$  and  $y$  for which the coefficients of the powers of  $x$  in  $F, G, D$  exist.

If  $b_0(y_0) \neq 0$  the algorithm is applicable and  $D(x, y_0)$  is a highest common factor of  $f(x, y_0)$  and  $g(x, y_0)$ . Since  $R(y_0) = 0$  and  $b_0(y_0) \neq 0$ ,  $f(x, y_0)$  and  $g(x, y_0)$  have a common root. Hence,  $D(x, y_0)$  is either identically zero or of positive degree in  $x$ .

But if  $D(x, y_0) \equiv 0$ , then  $g(x, y_0) \equiv 0$ , which is impossible since  $b_0(y_0) \neq 0$ .

Thus,  $D(x, y_0)$  is of positive degree in  $x$ . Therefore,  $D(x, y)$  is also.

If  $c(y)$  is a common denominator for the coefficients of the powers of  $x$  in  $F, G, D$ , then we may write

$$\begin{aligned} f(x, y) &= \frac{1}{c(y)} F_1(x, y)D_1(x, y) \\ g(x, y) &= \frac{1}{c(y)} G_1(x, y)D_1(x, y) \end{aligned}$$

where  $F_1(x, y), G_1(x, y), D_1(x, y)$  are polynomials in  $x$  and  $y$ . These equalities hold for all values of  $x$  and  $y$  for which  $c(y) \neq 0$ .

Since  $c(y)$  can vanish for only a finite number of values of  $y$  (possibly none), for any given value of  $x$

$$\begin{aligned}c(y)f(x, y) &= F_1(x, y)D_1(x, y) \\c(y)g(x, y) &= G_1(x, y)D_1(x, y)\end{aligned}$$

for infinitely many values of  $y$ . Since, for the given value of  $x$ , the right and left sides are polynomials in  $y$ , they are equal for all values of  $y$  (§4, Ch. 2). Hence, these equalities are identities holding for all values of  $x$  and  $y$ .

If  $c(y)$  is a constant, then  $D_1(x, y)$  is a common polynomial factor of  $f(x, y)$  and  $g(x, y)$  of positive degree in  $x$ . If not, let  $r$  be a root of  $c(y)$  and  $c(y) \equiv c_1(y)(y - r)$ . Consider  $D_1, F_1, G_1$  as polynomials in  $x$  with coefficients which are polynomials in  $y$ . Then (p. 12, §3, Ch. 11) either  $y - r$  is a factor of every coefficient in  $D_1$  or a factor of every coefficient in  $F_1$  and  $G_1$ . In either case

$$\begin{aligned}(y - r)c_1(y)f(x, y) &= (y - r)F_2(x, y)D_2(x, y) \\(y - r)c_1(y)g(x, y) &\equiv (y - r)G_2(x, y)D_2(x, y)\end{aligned}$$

where  $F_2, G_2, D_2$  are polynomials in  $x$  and  $y$ ,  $D_2$  of positive degree in  $x$ .

It follows, by canceling  $y - r$  (§3, Ch. 11), that

$$\begin{aligned}c_1(y)f(x, y) &= F_2(x, y)D_2(x, y) \\c_1(y)g(x, y) &\equiv G_2(x, y)D_2(x, y)\end{aligned}$$

If  $c_1(y)$  is a constant, the proof is complete. If not, we proceed as before.

After a number of such steps [equal to the degree of  $c(y)$ ], we arrive at the desired result.

*Example 1* Find all values of  $a$  for which

$$\begin{aligned}f(x, y) &= axy + (2a - 1)x + (1 - a)y + a - 1 \\g(x, y) &\equiv ay^2 + (2a - 1)y + (1 - a)x + 1 - a\end{aligned}$$

have a common factor of degree one or more.

The values of  $a$  for which there is a common factor of positive degree in  $x$  are those for which  $R(y) \equiv 0$ .

Eliminating  $x$  to obtain  $R(y)$ , we have

$$\begin{aligned}R(y) &\equiv \begin{vmatrix} ay + 2a - 1 & (1 - a)y + a - 1 \\ 1 - a & ay^2 + (2a - 1)y + 1 - a \end{vmatrix} \\&\equiv a(y + 1)[ay^2 + (3a - 2)y + 1 - a]\end{aligned}$$

$$R(y) \equiv 0 \text{ only for } a = 0.$$

For  $a = 0$  the polynomials are  $-x + y - 1$  and  $-y + x + 1$ , with an obvious common factor.

The values of  $a$  for which there is a common factor involving  $y$  (whether or not the factor also involves  $x$ ) are those which make the final equation in  $x$  an identity. Eliminating  $y$ , we have

$$\begin{aligned} R_1(x) &\equiv \begin{vmatrix} ax + 1 - a & (2a - 1)x + a - 1 & 0 \\ 0 & ax + 1 - a & (2a - 1)x + a - 1 \\ a & 2a - 1 & (1 - a)x + 1 - a \end{vmatrix} \\ &\equiv a(1 - a)[ax^3 - (a - 2)x^2 + (5 - 7a)x + 2 - 2a] \end{aligned}$$

which vanishes identically only when  $a$  is 0 or 1.

We have already taken care of the case  $a = 0$ .

For  $a = 1$  the polynomials are  $xy + x$  and  $y^2 + y$ , with  $y + 1$  as a common factor.

*Example 2* Find all the values of  $k$  for which  $xy - kx + (k - 1)y$  is reducible.

A polynomial is reducible if it is the product of two polynomials neither of which is a constant.

If it is reducible it has a factor of degree one. If the factor involves  $x$  we may suppose it has the form  $x + ay + b$ . To find when such a factor exists we ask: For what values of  $a$ ,  $b$ , and  $k$  does the resultant  $R(y)$  of  $xy - kx + (k - 1)y$  and  $x + ay + b$  vanish identically?

We have

$$R(y) \equiv \begin{vmatrix} y - k & (k - 1)y \\ 1 & ay + b \end{vmatrix} \equiv ay^2 + (1 + b - ak - k)y - bk$$

which vanishes identically if and only if

$$a = 0, 1 + b - ak - k = 0, -bk = 0.$$

Solving these equations for  $a$ ,  $b$ , and  $k$ , we find  $a = 0$ ,  $b = 0$ ,  $k = 1$  or  $a = 0$ ,  $b = -1$ ,  $k = 0$ .

For  $k = 1$  the given polynomial is  $xy - x \equiv x(y - 1)$ , and for  $k = 0$  it is  $xy - y \equiv (x - 1)y$ .

We must also seek the values of  $k$  for which the given polynomial has a factor which involves  $y$ . We leave it to the reader to show that we obtain again  $k = 0, 1$ .

## Exercises

- 1 For each of the following pairs of polynomials find a common factor of degree one or more or show that none exists.\* Also find the solutions of the systems of equations obtained by setting these polynomials equal to zero.

$$\begin{array}{ll} \text{a) } 4x^2 + 4x - y^2 + 1 & \text{c) } 2x^3 - 2x^2y - xy + y^2 + x - y \\ 4x^2 + 6xy - 4y^2 + 5y - 1 & x^3 + xy - 4x - x^2y - y^2 + 4y \\ \text{b) } x^2y - xy^2 - 2x^2 - 2x + 3xy & \text{d) } x^2y + xy^2 - y + 2x^2 + 2xy - 2 \\ x^3 + 2x^2 - xy^2 - 2y^2 & x^2y - xy^2 + y + 2x^2 - 2xy + 2 \end{array}$$

- 2 Find the values of  $a$  for which there is a common polynomial factor of degree one or more, and find such a factor for each such value of  $a$ :

$$\begin{array}{l} \text{a) } x^2 - ay^2 \\ x^3 - y^3 + ax^2 - xy^3 \\ \text{b) } (x - y)^2 + (a + 1)(x - y) + a \\ (x - y)^2 - (a + 1)(x - y) + a \\ \text{c) } y^3 - ax + axy - 1 \\ x^3y + 2xy^2 - a - ax^3 - 2axy + y \\ \text{d) } x^2 - xy - a + ax - x - ay \\ x^2 + 2xy + y^2 + (a + 1)(x + y) + a \\ \text{e) } x^2 + (a + 1)xy + ay^2 - ax - a^2y \\ x^3 + 3x^2y + 3xy^2 + y^3 - y - x \\ \text{f) } x^4 + x^3(a - y) + xy - y^2 + ay \\ x^2 + x(a - y + y^2) + ay^2 - y^3 \end{array}$$

- 3 Find the values of  $a$  for which the following are reducible:

$$\begin{array}{l} \text{a) } x^2 + x + ay^2 + y \\ \text{b) } x^2 - y^2 + 2ax + a \\ \text{c) } x^2 + xy + ay + (a - 2)x + a \\ \text{d) } x^2y + axy^2 + (2a - 3)x^2 - xy + (a - 1)y \\ \text{e) } x^2 - ay^2 + (1 - a)xy + a(a + 1)y - a^2 \\ \text{f) } xy + ax + y^3 + ay^2 + 1 \\ \text{g) } x^3 + ax^2 - 4xy^2 + 4ay^2 - 4x - 4a \end{array}$$

- 4 Prove: If  $f(x, y)$  and  $g(x, y)$  are non constant polynomials, at least one of positive degree in  $x$  and at least one of positive degree in  $y$ , and if the system  $f(x, y) = 0$ ,  $g(x, y) = 0$  has infinitely many solutions, then  $f(x, y)$  and  $g(x, y)$  have a common polynomial factor of degree one or more.
- 5 Prove: If  $f(x, y)$  vanishes whenever the (non-constant) irreducible polynomial  $g(x, y)$  does, then  $f(x, y) = g(x, y)h(x, y)$ . (Hint: Use ex. 4.)
- 6 Prove: If  $f(x, y)g(x, y)$  is divisible by the (non-constant) irreducible polynomial  $h(x, y)$ , then either  $f(x, y)$  or  $g(x, y)$  (or both) is divisible by  $h(x, y)$ . [Hint: Show that either  $f(x, y) = 0$ ,  $h(x, y) = 0$  or  $g(x, y) = 0$ ,  $h(x, y) = 0$  has infinitely many solutions; then use ex. 4.]

- 7 Prove. Every non-constant polynomial  $f(x, y)$  is uniquely factorable into irreducible factors. (Define "unique" factorization as in §12, Ch. 2.) (Hint: Use ex. 6.)
- 8 Prove: If  $f(x, y) \neq 0$ ,  $g(x, y) \neq 0$ , then there exists a highest common factor. (Define a H.C.F. as in §8, Ch. 2.) (Hint: Use ex. 7.)
- 9 A complex number is said to be algebraic if it is a root of a polynomial, not identically zero, with rational coefficients. Prove: If  $a + bi$  is algebraic then  $a$  and  $b$  are also. [Hint: Let  $a + bi$  be a root of  $f(x)$ . Let  $f(x + yi) = \varphi(x, y) + i\psi(x, y)$ . Eliminate  $a$  from  $\varphi(a, b) = 0$ ,  $\psi(a, b) = 0$  to show  $b$  algebraic.]

**7. Successive elimination** Suppose we seek the solutions, if any, of the system of three equations  $f(x, y) = 0$ ,  $g(x, y) = 0$ ,  $h(x, y) = 0$  in two unknowns, where  $f(x, y)$ ,  $g(x, y)$ , and  $h(x, y)$  are polynomials in  $x$  and  $y$ .

If we form the final equations  $R_{fg}(y) = 0$  and  $R_{gh}(y) = 0$  by eliminating  $x$  from  $f(x, y) = 0$ ,  $g(x, y) = 0$  and from  $g(x, y) = 0$ ,  $h(x, y) = 0$  respectively, we obtain two equations in  $y$  which must be satisfied by  $y$  whenever  $(x, y)$  is a solution of the given system.

If we eliminate  $y$  from these two equations we obtain a condition  $R = 0$  which must be satisfied if the given system has a solution.

The converse is not generally true. That is, it is possible that  $R = 0$  even though the given system has no solution.

In a similar way we can form the equations  $R_{fg}(y) = 0$  and  $R_{fh}(y) = 0$  and then, by eliminating  $y$ , obtain  $R' = 0$ .

We can also form the equations  $R_{gh}(y) = 0$  and  $R_{gh}(y) = 0$  and eliminate  $y$  to obtain  $R'' = 0$ .

If the given system has a solution it is necessary that all three conditions  $R = 0$ ,  $R' = 0$ ,  $R'' = 0$  hold. It is possible, however, that all three conditions hold without the system having a solution. Nevertheless, the information supplied by these conditions may enable us to determine whether there are any solutions and to find them.

**Example** Find the values of  $z$  for which

$$f(x, y, z) \equiv xy + xz - 2 = 0$$

$$g(x, y, z) \equiv y + xy - 2 = 0$$

$$h(x, y, z) \equiv yz - xy = 0$$

has a solution  $(x, y)$ .



Forming resultants by Sylvester's method, we have

$$\begin{aligned} R_{fa}(y) &= \begin{vmatrix} y+z & -2 \\ y & y-2 \end{vmatrix} \equiv y^2 + yz - 2z \\ R_{ah}(y) &= \begin{vmatrix} y & y-2 \\ -y & yz \end{vmatrix} \equiv y^2z + y^2 - 2y \\ R_{fh}(y) &= \begin{vmatrix} y+z & -2 \\ -y & yz \end{vmatrix} \equiv y^2z + yz - 2y \end{aligned}$$

Eliminating  $y$  from  $R_{fa}(y) = 0$ ,  $R_{fh}(y) = 0$ , we have

$$\begin{vmatrix} 1 & z & -2z & 0 \\ 0 & 1 & z & -2z \\ z & z^2 - 2 & 0 & 0 \\ 0 & z & z^2 - 2 & 0 \end{vmatrix} - 1z(z-1)(z^2 + 2z + 2) = 0$$

Eliminating  $y$  from  $R_{fa}(y) = 0$ ,  $R_{ah}(y) = 0$ , we have

$$\begin{vmatrix} 1 & z & -2z & 0 \\ 0 & 1 & z & -2z \\ 1+z & -2 & 0 & 0 \\ 0 & 1+z & -2 & 0 \end{vmatrix} - 1z(z-1)(z^2 + 2z + 2) = 0$$

Eliminating  $y$  from  $R_{ah}(y) = 0$ ,  $R_{fh}(y) = 0$ , we have

$$\begin{vmatrix} z & z^2 - 2 & 0 & 0 \\ 0 & z & z - 2 & 0 \\ 1+z & -2 & 0 & 0 \\ 0 & 1+z & -2 & 0 \end{vmatrix} = 0$$

Thus, the only values of  $z$  which there might be a solution  $(x, y)$  are the roots of  $1z(z-1)(z^2 + 2z + 2) = 0$ , or  $z = 0, 1, -1 + i, -1 - i$ .

For  $z = 0$  the equations are

$$\begin{aligned} xy - 2 &= 0 \\ y + xy - 2 &= 0 \\ xy &= 0 \end{aligned}$$

There is no solution since the first and last equations contradict each other

For  $z = 1$  the equations are

$$\begin{aligned} xy + x - 2 &= 0 \\ y + xy - 2 &= 0 \\ y - xy &= 0 \end{aligned}$$

By adding corresponding sides of the last two equations we obtain  $y = 1$ . The last equation then shows that  $x = 1$ . Direct substitution into the equations shows that  $(1, 1)$  satisfies all three.

Similarly, for  $z = -1 + i$  there is a unique solution  $(-1 + i, -2i)$  and for  $z = -1 - i$  a unique solution  $(-1 - i, 2i)$ .

If we regard the given system of equations as equations in the unknowns  $x, y, z$ , and  $(x_0, y_0, z_0)$  as a solution if the values  $x = x_0, y = y_0, z = z_0$  satisfy all the equations, then we have shown that the solutions are  $(1, 1, 1), (-1 + i, -2i, -1 + i), (-1 - i, 2i, -1 - i)$ .

### Exercises

Solve the following systems of equations:

a)  $x^2 - y^2 + 2 = 0$

$$y^2 - z^2 - 1 = 0$$

$$x - z + 1 = 0$$

b)  $x^2 - y = 1\frac{1}{2}$

$$y - z = 1$$

$$y^2 - z^2 = 2$$

c)  $xy = 2$

$$xz = 2$$

$$x^2 = y^2 + z^2 + 2$$

d)  $x - yz = 0$

$$y - xz = 0$$

$$z - xy = 0$$

e)  $xz - yz + z = 1$

$$x - y + z = 1$$

$$xz + yz - x - y - z = 0$$

f)  $x^2 + y - z = 0$

$$y^2 + x - z = 0$$

$$x + y + 1 = 0$$

g)  $x^2 + y - z = 0$

$$y^2 + x - z = 0$$

$$x + y - 1 = 0$$

# A P P E N D I X I

## MATHEMATICAL INDUCTION

**1. Principle of mathematical induction** The principle of mathematical induction may be stated roughly as follows: If a statement involving  $n$

- (1) is true when  $n = 1$ , and
- (2) whenever the statement is true for a positive integral value of  $n$ , say  $n = k$ , then it is also true for the succeeding value of  $n$ ,  $n = k + 1$ ,

then the statement is true for *all* positive integral values of  $n$ .

Although this is called the principle of mathematical induction, it has nothing to do with induction in the dictionary sense of the word. To reason inductively is to draw a general conclusion from specific data. Such reasoning is generally not valid, the conclusion not being one which must follow but only one which probably follows. Such reasoning is inadmissible in a logical development.

The principle of mathematical induction is not a mode of reasoning but a property of the system of positive integers which may be used, like any other property, to establish results involving these numbers. That this is so becomes clearer when we state the property more precisely, as follows:

*Principle of mathematical induction:* If a set of positive integers has the properties:

- (1) 1 is in the set
- (2) if  $k$  is in the set then  $k + 1$  is also,

then the set contains all the positive integers.

This is fairly evident intuitively. Actually it (or some equivalent form) is one of the axioms from which the structure of algebra and arithmetic is built.

*Example* Prove: If  $n$  is a positive integer, then  $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ .

*Proof:*

- (1) For  $n = 1$  the statement is  $1 = \frac{1(1+1)}{2}$ , which is true.
- (2) Suppose the statement is true for  $n = k$ . Then

$$1 + 2 + \cdots + k = \frac{k}{2}k(k+1)$$

(This is referred to as the hypothesis of the induction.)

For  $n = k + 1$ ,

$$\begin{aligned} 1 + 2 + \cdots + (k + 1) &= (1 + 2 + \cdots + k) + (k + 1) \\ &= \frac{1}{2}k(k + 1) + (k + 1) \\ &= \frac{1}{2}(k + 1)(k + 2) \end{aligned}$$

Thus, the statement is true for  $n = k + 1$ .

By the principle of mathematical induction, the desired result is established for all positive integral values of  $n$ .

To show more precisely that the principle of mathematical induction applies, let  $S$  be the set of positive integers for which the desired equality holds. We have shown: (1) 1 is in  $S$ , and (2) if  $k$  is in  $S$  then  $k + 1$  is also in  $S$ . Therefore, by the principle,  $S$  contains all the positive integers, i.e., the equality holds for all positive integral values of  $n$ .

**2. An equivalent property** The principle of mathematical induction is equivalent to:

*Property (a)* In any set (finite or infinite) of positive integers there is a smallest.

We show:

(1) Property (a) follows from the principle of mathematical induction.

Let  $S$  be the given set. Proceeding by the indirect method, suppose  $S$  has no smallest integer.

1 is not in  $S$ , for if it were it would be the smallest integer in  $S$ .

Let  $T$  be the set consisting of those positive integers  $n$  with the property that all the integers in  $S$  exceed  $n$ .

We have already seen that 1 is in  $T$ .

Suppose  $k$  is in  $T$ . Then every integer in  $S$  exceeds  $k$ . If  $k + 1$  were in  $S$  it would be the smallest integer in  $S$ , contradicting the assumption that  $S$  has no smallest. Thus,  $k + 1$  is not in  $S$ . Hence, every integer in  $S$  exceeds  $k + 1$ . Therefore,  $k + 1$  is in  $T$ .

By the principle of mathematical induction,  $T$  contains all the positive integers.

This is impossible; for, if  $p$  is in  $S$ ,  $p$  is not in  $T$ .

This contradiction establishes the desired result.

(2) The principle of mathematical induction follows from property (a).

Let  $S$  be a set of positive integers containing 1 and such that  $k + 1$  is in  $S$  whenever  $k$  is.

If  $S$  does not contain all the positive integers, let  $T$  be the set of those positive integers which are not in  $S$ . By property (a) there is a smallest integer,  $p$ , in  $T$ .

Since 1 is in  $S$ ,  $p > 1$ .

Since  $p$  is the smallest positive integer not in  $S$ ,  $p - 1$  is in  $S$ . Hence, by hypothesis,  $p$  is also in  $S$ . Since  $p$  is in  $T$ , this is impossible.

This contradiction shows that  $S$  must contain all the positive integers.

**3. Other forms of the principle** The principle of mathematical induction may be stated in other useful forms. (Throughout the text these, as well as the statement in §1, are referred to indiscriminately as the principle of mathematical induction.)

Let  $S$  be a set of integers (not necessarily all positive).

- (b) If  $S$  contains 1 and contains  $k + 1$  whenever it contains  $1, 2, \dots, k$ , then  $S$  contains all the positive integers.
- (c) If  $S$  contains  $\lambda$  (positive, negative, or zero) and contains  $k + 1$  whenever it contains  $k$ , where  $k \geq \lambda$ , then  $S$  contains all the integers equal to or greater than  $\lambda$ .
- (d) If  $S$  contains  $\lambda$  and contains  $k + 1$  whenever it contains  $\lambda, \lambda + 1, \dots, k$ , where  $k \geq \lambda$ , then  $S$  contains all the integers equal to or greater than  $\lambda$ .
- (e) If  $S$  contains 1 and contains  $k + 1$  whenever it contains  $k < \alpha$  (where  $\alpha$  is a given positive integer), then  $S$  contains  $1, 2, \dots, \alpha$ .
- (f) If  $S$  contains 1 and contains  $k + 1$  whenever it contains  $1, 2, \dots, k$ , where  $k < \alpha$ , then  $S$  contains  $1, 2, \dots, \alpha$ .

Each of these is equivalent to the form of the principle as stated in §1, or to property (a). We illustrate with (d), leaving to the reader the proofs of the equivalence of the other forms.

Suppose  $S$  contains  $\lambda$  and contains  $k + 1$  whenever it contains  $\lambda, \lambda + 1, \dots, k$ , where  $k \geq \lambda$ .

Suppose there is an integer  $p > \lambda$  not in  $S$ . Let  $T$  be the set of all positive integers  $n$  such that  $n + (\lambda - 1)$  is not in  $S$ . Then  $T$  contains  $p - (\lambda - 1)$ , for  $p - (\lambda - 1) > 0$  and  $[p - (\lambda - 1)] + (\lambda - 1) = p$  is not in  $S$ .

By property (a), there is a smallest integer  $r$  in  $T$ .

Since  $1 + (\lambda - 1) = \lambda$  is in  $S$ , 1 is not in  $T$ . Hence,  $r \geq 2$ .

Since  $1, 2, \dots, r - 1$  are not in  $T$ ,  $1 + (\lambda - 1) = \lambda, 2 + (\lambda - 1) = \lambda + 1, \dots, (r - 1) + (\lambda - 1) = r + \lambda - 2$  are in  $S$ . Therefore, by hypothesis,  $(r + \lambda - 2) + 1 = r + (\lambda - 1)$  is also in  $S$ . Hence,  $r$  is not in  $T$ .

Since  $r$  is in  $T$ , we have a contradiction, which shows that there cannot be an integer greater than  $\lambda$  which is not in  $S$ . Thus, the desired result is established.

[Incidentally, by taking  $\lambda = 1$ , this also proves (b).]

Conversely, property (a) follows from (d). The proof is the same as part (1) in §2.

**Example 1** Prove: For every positive integer  $n$ ,  $n + 1$  is a prime or can be factored into primes.

(An integer greater than 1 is a prime if it is not the product of two positive integers neither of which is 1.)

*Proof:* Since 2 is a prime, the statement is true for  $n = 1$ .

We assume, as the hypothesis of the induction, that the statement is true for  $n = 1, 2, \dots, k$ , i.e., that each of  $2, 3, \dots, k + 1$  is a prime

or can be factored into primes. We show that the statement is true for  $n = k + 1$ .

If  $k + 2$  is a prime, there is nothing more to be proved. If not, then  $k + 2 = pq$ , where  $p$  and  $q$  are positive integers neither equal to 1.

Since  $q > 1$ ,  $p$  is less than  $k + 2$ . Hence, the hypothesis of the induction applies to  $p$ . Thus,  $p$  is a prime or can be factored into primes.

Similarly,  $q$  is a prime or can be factored into primes.

Thus,  $k + 2 = pq$  can be factored into primes.

Therefore, the truth of the statement has been established for  $n = k + 1$ .

It follows from (b) above that the statement is true for all positive integral values of  $n$ .

*Remark* In this proof we could not have used the principle as stated in §1, since we cannot say that  $p = k + 1$  or  $q = k + 1$ .

It will often be found that (b) is more useful than the statement in §1. In applying the latter we have to show: The hypothesis that  $S$  contains  $k$  implies that  $S$  contains  $k + 1$ . In applying (b) we have to show: The hypothesis that  $S$  contains 1, 2,  $\dots$ ,  $k$  implies that  $S$  contains  $k + 1$ . The usefulness of (b) lies in the fact that the second hypothesis contains more information than the first.

*Example 2* Show that  $(\frac{3}{2})^n > 1 + n$  for  $n \geq 4$ .

For  $n = 4$  the statement is true, since  $(\frac{3}{2})^4 > 1 + 4$ .

Assume, as the hypothesis of the induction, that the statement is true for  $n = k \geq 4$ . Then, for  $n = k + 1$ ,

$$\begin{aligned} (\frac{3}{2})^{k+1} &= (\frac{3}{2})^k \cdot \frac{3}{2} > (1 + k) \cdot \frac{3}{2} \quad (\text{by the hypothesis of the induction}) \\ &= (1 + k) + \frac{1}{2}(1 + k) \geq (1 + k) + \frac{1}{2}(1 + 4) > (1 + k) + 1 \\ &= 1 + (k + 1) \end{aligned}$$

which proves the statement for  $n = k + 1$ .

By (c) above, the statement is true for all  $n \geq 4$ .

### Exercises

If  $n$  is a positive integer, prove:

$$1 \cdot 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{for } n \geq 1.$$

$$2 \cdot \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1} \quad \text{for } n \geq 1.$$

$$3 \cdot 1 + r + r^2 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1} \quad \text{for } n \geq 1, r \neq 1.$$

$$4 \cdot (1 + a)^n \geq 1 + na \quad \text{for } n \geq 1, a > 0$$

$$5 \cdot (n + 1)^3 > 27n \quad \text{for } n > 3$$

$$6 \cdot n^3 + 1 > n^3 + n \quad \text{for } n \geq 2$$

$$7 \cdot 8^n - 3^n \text{ has 5 as a factor if } n \geq 1$$

$$8 \cdot n^3 - n \text{ has 3 as a factor if } n > 1$$

- 9 The maximum number of lines determined by  $n > 1$  points is  $\frac{1}{2}n(n-1)$ .
- 10 The maximum number of points of intersection of  $n \geq 2$  lines is  $\frac{1}{2}n(n-1)$ .
- 11 The sum of the angles of an  $n$ -sided polygon is  $(n-2)180^\circ$ .
- 12 If an amount of money  $P$  is invested at an annual interest rate  $r$  and interest is compounded annually, after  $n$  years the sum amounts to  $P(1+r)^n$ .
- 13 The number of positive prime factors of  $n \geq 2$  is less than  $2 \log_e n$ .
- 14 In a set of  $n$  distinct integers there is a greatest.
- 15 If  $1 + 2 + \cdots + n = \frac{1}{2}(n+1)^2$  is true for  $n = k \geq 1$  it is true for  $n = k+1$ , but the equality does not hold for all values of  $n$ .

## A P P E N D I X I I

### SOLUTIONS OF STARRED EXERCISES

The results contained in the starred exercises constitute an integral part of the text since they are used in proving later theorems or in establishing important methods. This Appendix contains outlines of their proofs.

Those exercises to which reference is made (in remarks, examples, etc.) but which are not required in establishing essential results have not been starred.

#### CHAPTER 2

§4, ex. 17 (Used in §3, Ch. 4)

If  $n = 0$ ,  $f_0(x)$  is a non-zero constant and  $F(x)$  is a constant. Hence,  $F(x) = c_0 f_0(x)$ .

Assume the result for  $n \leq k$ . Let  $n = k + 1$ ,

$$\begin{aligned} F(x) &= a_0 x^{k+1} + a_1 x^k + \cdots + a_{k+1} \\ f_{k+1}(x) &\equiv b_0 x^{k+1} + b_1 x^k + \cdots + b_{k+1}, \quad b_0 \neq 0 \end{aligned}$$

Then  $F(x) - (a_0/b_0)f_{k+1}(x)$  is identically zero or of degree at most  $k$ . By the hypothesis of the induction,

$$F(x) - \frac{a_0}{b_0} f_{k+1}(x) \equiv c_0 f_0(x) + c_1 f_1(x) + \cdots + c_k f_k(x)$$

which establishes the desired result for  $n = k + 1$ .

To establish the uniqueness, suppose

$$c_0 f_0(x) + c_1 f_1(x) + \cdots + c_n f_n(x) \equiv d_0 f_0(x) + d_1 f_1(x) + \cdots + d_n f_n(x).$$

Then  $(c_0 - d_0)f_0(x) + (c_1 - d_1)f_1(x) + \cdots + (c_n - d_n)f_n(x) \equiv 0$ .

If not all the  $c_i - d_i = 0$ , the degree of the left side is the largest value of  $i$  for which  $c_i \neq d_i$ . This is impossible since the zero polynomial has no degree. Hence,  $c_i - d_i = 0$  for every  $i$ .

§4, ex. 21 (Used in §7, Ch. 7)

(a) Since  $f(x) - f(a)$  vanishes for  $x = a$ , by the factor theorem  $f(x) - f(a) \equiv (x - a)g(x)$ .

If  $|x - a| < \lambda$ , then  $x = (x - a) + a$ ,  $|x| \leq |x - a| + |a| < \lambda + |a| = \mu$ .



If  $g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$ , then for  $|x - a| < \lambda$ ,  $|g(x)| \leq |b_0x^n| + |b_1x^{n-1}| + \cdots + |b_{n-1}x| + |b_n| \leq |b_0|\mu^n + |b_1|\mu^{n-1} + \cdots + |b_{n-1}|\mu + |b_n| = M$ .

Hence,  $|f(x) - f(a)| \leq |x - a|M$ .

(b) Choose  $\delta > 0$  so that  $\delta M < \epsilon$ . Then for  $|x - a| < \delta$ ,  $|f(x) - f(a)| \leq |x - a|M \leq \delta M < \epsilon$ .

§5, ex. 2 (The fact that 0 and 1 are in every field is used in §4, Ch. 10)

If  $a \neq 0$  is in  $\mathfrak{F}$ , then  $a - a = 0$  and  $a/a = 1$  are also in  $\mathfrak{F}$ .

§5, ex. 9 (The fact that  $a_0\lambda^n + a_1\lambda^{n-1} + \cdots + a_n$  is in  $\mathfrak{F}$  is used in §5, Ch. 10)

For  $n = 0$  it is obvious. Suppose it true for  $n = k$ . Let  $n = k + 1$ .

By the hypothesis of the induction,  $a_0\lambda^k + a_1\lambda^{k-1} + \cdots + a_k$  is in  $\mathfrak{F}$ . Hence  $\lambda(a_0\lambda^k + a_1\lambda^{k-1} + \cdots + a_k)$  is in  $\mathfrak{F}$ . Therefore,  $\lambda(a_0\lambda^k + a_1\lambda^{k-1} + \cdots + a_k) + a_{k+1}$  is in  $\mathfrak{F}$ , which establishes the desired result for  $n = k + 1$ .

§7, ex. 6 (Used in §12, Ch. 2)

If  $f = ag$ ,  $g = bh$ , where  $a$  and  $b$  are constants in  $\mathfrak{F}$ , then  $f = (ab)h$  and  $ab$  is a constant in  $\mathfrak{F}$ .

§10, ex. 5 [Used in §2, Ch. 5 for  $m = 1$  and  $f$  and  $g$  integers (see §13, Ch. 2)]

Let  $f$  and  $g$  be polynomials,  $m = 1$ .

For  $n = 1$ ,  $f$  and  $g$  are relatively prime. Suppose  $f^k$  and  $g$  are,  $k \geq 1$ . Then (§10, Ch. 2),  $Af^k + Bg = 1$ . Multiplying by  $f$ , we have  $f \equiv Af^{k+1} + (Bf)g$ . Thus, every common factor of  $f^{k+1}$  and  $g$  is a factor of  $f$  (and  $g$ ). Since  $f$  and  $g$  are relatively prime, every common factor of  $f$  and  $g$ , and therefore also of  $f^{k+1}$  and  $g$ , is a constant.

This establishes the desired result for  $n = k + 1$ .

§10, ex. 9 (Used in ex. 13, §11, Ch. 2. Also used, for integers [see §13, Ch. 2], in §2, Ch. 5 and §6, Ch. 10)

Since  $f$  and  $h$  are relatively prime,  $Af + Bh = 1$  (§10, Ch. 2). Multiplying by  $g$ ,  $g \equiv Afg + Bgh$ . Since each term on the right has  $h$  as a factor,  $h$  is a factor of  $g$ .

§10, ex. 10 (Used in §3, Ch. 14)

Let  $D$  be a H.C.F. of  $f$  and  $g$  and  $D \equiv Af + B'g$  (§9, Ch. 2). Then  $BD \equiv BA'f + BB'g \equiv RA'f - B'Af \equiv (RA' - B'A)f$ .

$BA' - B'A \neq 0$  since  $BD \neq 0$ . Hence, the degree of the right side is  $n$  or greater. Since the degree of  $B$  is  $n - p$  or less, the degree of  $D$  is at least  $p$ .

## §11, ex. 9 (Used in §12, Ch. 2)

Suppose  $f(x)$  irreducible,  $f_1(x) \equiv cf(x)$ ,  $c$  a non-zero constant in  $\mathfrak{F}$ .

If  $f_1(x) \equiv g(x)h(x)$

then  $f(x) \equiv \left[ \frac{1}{c} g(x) \right] h(x)$

Hence, either  $h(x)$  or  $(1/c)g(x)$  is a constant. Therefore,  $h(x)$  or  $g(x)$  is a constant.

## §11, ex. 11 (Used in §12, Ch. 2)

If they are not relatively prime, they have a common factor  $h(x)$  in  $\mathfrak{F}[x]$  of degree one or more. Since  $f(x)$  and  $g(x)$  are primes over  $\mathfrak{F}$ ,  $h(x)$  is an associate of each. If  $h(x) \equiv af(x) \equiv bg(x)$ ,  $a$  and  $b$  non-zero constants in  $\mathfrak{F}$ , then  $g(x) \equiv (a/b)f(x)$ . Thus,  $g(x)$  is an associate of  $f(x)$ .

## §11, ex. 13 (Used in §12, Ch. 2)

For  $n = 1$  it is obvious. Suppose it true for  $n = k$ . Let  $n = k + 1$ .

Let  $g(x) \equiv f_1(x)f_2(x) \cdots f_k(x)$ . By hypothesis,  $f(x)$  divides  $g(x)f_{k+1}(x)$ .

If  $f(x)$  is prime to  $f_{k+1}(x)$ , it divides  $g(x)$  (ex. 9, §10, Ch. 2). Therefore, by the hypothesis of the induction, it divides one of  $f_1(x)$ ,  $f_2(x)$ ,  $\dots$ ,  $f_k(x)$ .

If  $f(x)$  is not prime to  $f_{k+1}(x)$ , some non-constant factor of  $f(x)$  divides  $f_{k+1}(x)$ . But  $f(x)$  is irreducible over  $\mathfrak{F}$ , so that its only non-constant factors in  $\mathfrak{F}[x]$  are its associates. Hence,  $f_{k+1}(x)$  is divisible by an associate of  $f(x)$  and, therefore, by  $f(x)$ .

## §13, ex. 5 (Used in §6, Ch. 10)

(a) If they are not all distinct, let  $\omega^i$  be the first one which is equal to a preceding one. Then  $\omega^i = \omega^j$  where  $0 \leq i < j \leq p - 1$ . Hence,  $\omega^{j-i} = 1 = \omega^0$ .

If  $i \neq 0$ , then  $\omega^{j-i}$  is a power of  $\omega$  which precedes  $\omega^j$  and which repeats a preceding power of  $\omega$ . By definition of  $j$ , this is impossible. Hence,  $i = 0$ , so that  $\omega^j = \omega^0 = 1$ .

If  $p = qj + r$  where  $0 \leq r < j$ , then  $\omega^0 = 1 = \omega^p = \omega^{qj+r} = (\omega^j)^q \omega^r = \omega^r$ . This is impossible since  $r < j$ .

(b) Each is a  $p$ th root of  $a$ , since  $(\alpha\omega^i)^p = \alpha^p(\omega^p)^i = \alpha^p = a$ .

No two are equal. For, if  $\alpha\omega^i = \alpha\omega^j$  then  $\omega^i = \omega^j$ , which is impossible by (a).

They are all the  $p$ th roots of  $a$  since  $x^p - a$  cannot have more than  $p$  roots.

## §13, ex. 6 (Used in §7, Ch. 10)

If  $r = 1$  the desired result is obvious with each  $b_i = 1$ . Suppose it true for  $r = 1, 2, \dots, k$  and let  $r = k + 1$ .

If  $p$  is a positive prime factor of  $r$ ,  $p$  is a factor of some  $a_i$ , say  $a_1$ . By hypothesis,  $a_1 a_2 \cdots a_n = br$ . Hence,  $(a'_1 p) a_2 \cdots a_n = b(r'p)$ , so that  $a'_1 a_2 \cdots a_n = br'$ .

Since  $r'$  is a factor of  $a'_1 a_2 \cdots a_n$  and  $r' < k + 1$ , by the hypothesis of the induction  $r' = b'_1 b_2 \cdots b_n$  where  $b'_1$  is a factor of  $a'_1$  and  $b_i$  is a factor  $a_i$  for  $i = 2, 3, \dots, n$ .

Hence,  $r = pr' = (pb'_1) b_2 \cdots b_n = b_1 b_2 \cdots b_n$ , where  $b_i$  is a factor of  $a_i$  for  $i = 1, 2, \dots, n$ .

## CHAPTER 4

§1, ex. 5 (The second part is used in §2 and §4, Ch. 4, and §6, Ch. 5. This follows from the first part by letting  $f(x) = x - a$ )

For  $m = 1$  it is obvious. Assume it for  $m = k$ . Then

$$\begin{aligned} [f^{k+1}(x)]' &\equiv [f^k(x)f(x)]' = [f^k(x)]'f(x) + f^k(x)f'(x) \\ &\equiv [kf^{k-1}(x)f'(x)]f(x) + f^k(x)f'(x) \\ &\equiv (k+1)f^k(x)f'(x) \end{aligned}$$

## CHAPTER 5

§2, ex. 15 (Used in §6, Ch. 10)

Let  $f(x)$  be a factor of  $x^n - a$  of degree  $m > 0$  with coefficients in  $\mathfrak{F}$  and leading coefficient 1, with the roots  $r_1, r_2, \dots, r_m$ . Then  $r = r_1 r_2 \cdots r_m = (-1)^m \alpha$  where  $\alpha$  is the constant term in  $f(x)$ . Hence,  $r$  is in  $\mathfrak{F}$ .

Since each  $r_i$  is a root of  $x^n - a$ ,  $r^n = r_1^n r_2^n \cdots r_m^n = \alpha^n \cdots \alpha^n = \alpha^m$ .

If  $m < n$  then, since  $n$  is a prime,  $m$  and  $n$  are relatively prime. Hence  $\lambda n + \mu m = 1$  (§13, Ch. 2). Therefore,

$$(a^{\lambda} r^{\mu})^n = a^{n\lambda} (r^n)^{\mu} = a^{n\lambda} (\alpha^m)^{\mu} = a^{n\lambda + \mu m} = a$$

Thus,  $a$  has an  $n$ th root,  $a^{\lambda} r^{\mu}$ , in  $\mathfrak{F}$ , contrary to the hypothesis.

Hence,  $m = n$ . Therefore, the other factor of  $x^n - a$  is a constant.

§7, ex. 3 (Used in §7, Ch. 7)

$\varphi(a) = \varphi(b) = 0$ . Suppose  $\varphi(x) \neq 0$ . Then  $\varphi(x)$  has a finite number of roots in  $[a, b]$ . Therefore, it has two consecutive roots in the interval.

Since  $g(x)$  is never zero in  $[a, b]$ , by the location principle it has the same sign for every  $x$  in the interval.

By the theorem of §6, Ch. 5,

$$g(x)\varphi'(x) - g'(x)\varphi(x) \equiv g(x)f'(x) - f(x)g'(x) - \left[ \frac{f(b)}{g(b)} - \frac{f(a)}{g(a)} \right] \frac{g^2(x)}{b-a}$$

vanishes for  $x = x_0$ , where  $x_0$  is between  $a$  and  $b$ .

Letting  $x = x_0$ , setting the right side equal to zero, and solving for  $[f(b)/g(b)] - [f(a)/g(a)]$ , establishes the desired result.

If  $\varphi(x) \equiv 0$ , then  $g(x)\varphi'(x) - g'(x)\varphi(x) \equiv 0$ . Hence, this certainly vanishes for any  $x_0$  between  $a$  and  $b$ , and the desired result again follows.

§7, ex. 5 (Used in §7, Ch. 7)

By the location principle,  $f(x)$  is always positive or always negative in  $[a, b]$ . Suppose it is positive.

If  $f'(x) \equiv 0$ ,  $f(x)$  is a positive constant. Hence, an  $M$  exists.

Suppose  $f'(x) \neq 0$ .

If  $f'(x)$  has no root between  $a$  and  $b$ , it is always positive or always negative for  $a < x < b$ . Hence,  $f(x)$  is monotonically increasing or monotonically decreasing in  $[a, b]$ . In the first case  $f(x) \geq f(a) > 0$  for every  $x$  in  $[a, b]$  and in the second  $f(x) \geq f(b) > 0$ . In the first case let  $0 < M < f(a)$  and in the second  $0 < M < f(b)$ .

If  $f'(x)$  has one or more roots between  $a$  and  $b$ , let them be  $r_1, r_2, \dots, r_m$  arranged according to increasing magnitude. Let  $r_0 = a$ ,  $r_{m+1} = b$ . Then  $r_0 < r_1 < \dots < r_m < r_{m+1}$ .

$f'(x)$  has no root between  $r_{i-1}$  and  $r_i$  ( $i = 1, 2, \dots, m+1$ ). Hence, from the preceding,  $f(x) > M_i$  for  $x$  in  $[r_{i-1}, r_i]$ . We have only to take  $M$  as the smallest of the  $M_i$ .

If  $f(x)$  is negative in  $[a, b]$ , then  $g(x) \equiv -f(x)$  is positive. Hence, as already proved,  $g(x) > M$ . Therefore,  $f(x) < -M$ .

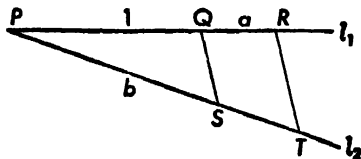
## CHAPTER 9

§1, ex. 2 (Parts a, b, c, d, e are used in §2, Ch. 9)

(a) and (b) are obvious.

(c) Through any point  $P$  draw two rays  $l_1$  and  $l_2$  making an acute angle. On  $l_1$  lay off  $PQ = 1$ ,  $QR = a$ . On  $l_2$  make  $PS = b$ . Draw  $RT$  parallel to  $QS$ . (This is a ruler and compass construction.) Then,

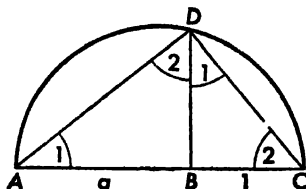
$$\frac{ST}{QR} = \frac{PS}{PQ}, \quad \frac{ST}{a} = \frac{b}{1}, \quad ST = ab$$



(d) To construct  $a/b$  proceed as in (c), making  $PQ = b$ ,  $QR = a$ ,  $PS = 1$ . Then  $ST = a/b$ .

(e) To construct  $\sqrt{a}$ , in the accompanying diagram make  $AB = a$ ,  $BC = 1$ . Draw a semicircle with  $AC$  as diameter. Draw  $BD$  perpen-

dicular to  $AC$ . Then  $\angle ADC = 90^\circ$ . Triangles  $ABD$  and  $BCD$  are similar. Hence  $BD/BC = AB/BD$ ,  $\overline{BD}^2 = BC \cdot AB = a$ ,  $BD = \sqrt{a}$ .



§1, ex. 3 (Used in §2, Ch. 9)

Let  $B_1, B_2, \dots, B_n$  be a succession of configurations, each obtained from the preceding ones in the manner described in §1, Ch. 9, with  $B_1 = B$ , which include all the figures in  $A$ . Let  $C_1, C_2, \dots, C_m$  be a similar succession of configurations with  $C_1 = C$ , including the figure of  $B$ . Then  $C_1, \dots, C_m, B_1, \dots, B_n$  is a succession of configurations, each obtainable from the preceding ones in the required manner, including all the figures in  $A$ .

§2, ex. 1 (Used in §5, Ch. 9)

Let  $c_1, c_2, \dots, c_p$ , where  $c_p = c$ , be a sequence in which every  $c$  is one of  $b_1, b_2, \dots, b_m$  or is a sum, product, difference, or quotient of preceding  $c$ 's.

For  $i = 1, 2, \dots, m$ , let  $a_{i1}, a_{i2}, \dots, a_{ip_i}$  be a sequence in which  $a_{ip_i} = b_i$  and each  $a$  is one of  $a_1, a_2, \dots$ , or is a sum, product, difference, or quotient of preceding  $a$ 's in the sequence.

Then  $a_{11}, a_{12}, \dots, a_{1p_1}, a_{21}, a_{22}, \dots, a_{2p_2}, \dots, a_{m1}, a_{m2}, \dots, a_{mp_m}, c_1, c_2, \dots, c_p$  is a sequence of the required type in which  $c_p = c$ .

§2, ex. 2 (Used in §2 and 7, Ch. 9, and in ex. 3, §2, Ch. 9)

Proof similar to that in preceding exercise.

§2, ex. 3 (Used in §7, Ch. 9)

Since  $x = (-b \pm \sqrt{b^2 - 4ac})/2a$ ,  $x$  is obtainable from  $a, b, c$  by rational operations and extractions of square roots. The desired result now follows by applying the preceding exercise.

## CHAPTER 10

§1, ex. 7 (If  $\xi$  is in  $\mathfrak{F}$  then it is of degree one over  $\mathfrak{F}$  is used in §6, Ch. 10)

This is obvious since  $\xi$  is a root of  $x - \xi$  which has coefficients in  $\mathfrak{F}$  and is irreducible over  $\mathfrak{F}$ .

§3, ex. 15 (Used in §5, 6, 7 and in ex. 15, §5, Ch. 10)

If  $\xi$  is in  $\mathcal{K}$ , then  $\xi = a_1 u_1 + \cdots + a_n u_n$ , the  $a_i$  in  $\mathcal{L}$ .

Also,  $a_i = c_{i1} v_1 + \cdots + c_{im} v_m$  ( $i = 1, 2, \cdots, n$ ), the  $c_{ij}$  in  $\mathcal{F}$ .

Hence,

$$\begin{aligned}\xi &= (c_{11} v_1 + \cdots + c_{1m} v_m) u_1 + \cdots + (c_{n1} v_1 + \cdots + c_{nm} v_m) u_n \\ &= c_{11} u_1 v_1 + \cdots + c_{1m} u_1 v_m + \cdots + c_{n1} u_n v_1 + \cdots + c_{nm} u_n v_m\end{aligned}$$

To show this unique, suppose also

$$\xi = d_{11} u_1 v_1 + \cdots + d_{1m} u_1 v_m + \cdots + d_{n1} u_n v_1 + \cdots + d_{nm} u_n v_m, \text{ the } d_i \text{ in } \mathcal{F}.$$

By equating the two expressions for  $\xi$  and rearranging terms,

$$\begin{aligned}(c_{11} v_1 + \cdots + c_{1m} v_m) u_1 + \cdots + (c_{n1} v_1 + \cdots + c_{nm} v_m) u_n \\ = (d_{11} v_1 + \cdots + d_{1m} v_m) u_1 + \cdots + (d_{n1} v_1 + \cdots + d_{nm} v_m) u_n\end{aligned}$$

The  $c$ 's,  $d$ 's,  $n$ 's are in  $\mathcal{L}$ . Hence, the multipliers of the  $u$ 's are in  $\mathcal{L}$ . Because of the unique expressibility of the numbers in  $\mathcal{K}$  in terms of the basis  $u_1, \cdots, u_n$ ,

$$\begin{array}{ccccccc}c_{11} v_1 & + & \cdots & + & c_{1m} v_m & = & d_{11} v_1 + \cdots + d_{1m} v_m \\ \vdots & & \vdots & & \vdots & & \vdots \\ c_{n1} v_1 & + & \cdots & + & c_{nm} v_m & = & d_{n1} v_1 + \cdots + d_{nm} v_m\end{array}$$

Because of the unique expressibility of the numbers in  $\mathcal{L}$  in terms of the basis  $v_1, \cdots, v_m$ ,  $c_{ij} = d_{ij}$  for all  $i$  and  $j$ .

§3, cr. 16 (That  $\mathcal{K}$  is of finite degree over  $\mathcal{L}$  is used in ex. 15, §5, Ch. 10)

Let  $u_1, \cdots, u_n$  be a basis for  $\mathcal{K}$  over  $\mathcal{F}$ . Then every number in  $\mathcal{K}$  has the form  $c_1 u_1 + \cdots + c_n u_n$  with  $c$ 's in  $\mathcal{L}$  (since this is true with  $c$ 's in  $\mathcal{F}$ ).

Let  $k \leq n$  be the smallest value of  $m$  for which there exists a set of  $m$   $u$ 's such that every number in  $\mathcal{K}$  is expressible in this form, with  $c$ 's in  $\mathcal{L}$ , using only these  $m$   $u$ 's. To be specific, suppose  $u_1, \cdots, u_k$  are such  $u$ 's.

We show that every such expression is unique, i.e., if  $c_1 u_1 + \cdots + c_k u_k = d_1 u_1 + \cdots + d_k u_k$  with  $c$ 's and  $d$ 's in  $\mathcal{L}$ , then  $c_i = d_i$  ( $i = 1, 2, \cdots, k$ ).

From the equality,  $(c_1 - d_1) u_1 + \cdots + (c_k - d_k) u_k = 0$ .

If  $k = 1$ , then  $(c_1 - d_1) u_1 = 0$ . If  $c_1 - d_1 \neq 0$ , then  $u_1 = 0$ , so that every number in  $\mathcal{K}$  is zero. This is impossible.

If  $k > 1$  and not every  $c_i - d_i$  is zero, suppose, to be specific,  $c_k - d_k \neq 0$ . Then  $u_k = a_1 u_1 + \cdots + a_{k-1} u_{k-1}$  where  $a_i = -\frac{(c_i - d_i)}{c_k - d_k}$ .

The  $a_i$  are in  $\mathcal{L}$ .

Thus, every number in  $\mathcal{K}$  has the form

$$\begin{aligned} c_1 u_1 + \cdots + c_k u_k &= c_1 u_1 + \cdots + c_{k-1} u_{k-1} \\ &\quad + c_k (a_1 u_1 + \cdots + a_{k-1} u_{k-1}) \\ &= b_1 u_1 + \cdots + b_{k-1} u_{k-1} \end{aligned}$$

with  $b$ 's in  $\mathcal{L}$ .

This is a contradiction, since  $k$  is the smallest number of  $u$ 's for which this is possible.

Thus,  $u_1, \dots, u_k$  is a basis for  $\mathcal{K}$  over  $\mathcal{L}$ .

§5, ex. 15 (Used in §6 and §7, Ch. 10)

Since  $\mathcal{K}$  contains  $\mathcal{F}$  and  $a$ , it contains  $\mathcal{F}(a)$ .

Since  $\mathcal{K}$  is of finite degree over  $\mathcal{F}$ , it is of finite degree over  $\mathcal{F}(a)$  (ex. 16, §3, Ch. 10). Let  $\mathcal{K}$  be of degree  $p$  over  $\mathcal{F}(a)$ . Since  $\mathcal{F}(a)$  is of degree  $m$  over  $\mathcal{F}$  (§5, Ch. 10),  $\mathcal{K}$  is of degree  $pm$  over  $\mathcal{F}$  (ex. 15, §3, Ch. 10). Hence,  $pm = n$ .

## CHAPTER 11

§2, ex. 1 (Used in §5, Ch. 11)

Let  $n > 1$ . By arranging the terms in  $f(x_1, \dots, x_n)$  according to powers of  $x_n$ ,

$$f \equiv f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n + \cdots + f_p(x_1, \dots, x_{n-1})x_n^p$$

Suppose also

$$f \equiv g_0(x_1, \dots, x_{n-1}) + g_1(x_1, \dots, x_{n-1})x_n + \cdots + g_q(x_1, \dots, x_{n-1})x_n^q$$

where  $q \geq p$ .

If  $a_1, \dots, a_{n-1}$  are any values of  $x_1, \dots, x_{n-1}$ , then

$$\begin{aligned} f_0(a_1, \dots, a_{n-1}) + f_1(a_1, \dots, a_{n-1})x_n + \cdots + f_p(a_1, \dots, a_{n-1})x_n^p \\ = g_0(a_1, \dots, a_{n-1}) + g_1(a_1, \dots, a_{n-1})x_n + \cdots \\ + g_q(a_1, \dots, a_{n-1})x_n^q \end{aligned}$$

for all values of  $x_n$ .

Therefore (§4, Ch. 2),

$$\begin{aligned} g_i(a_1, \dots, a_{n-1}) &= 0 \quad \text{for } i > p \\ &= f_i(a_1, \dots, a_{n-1}) \quad \text{for } i = 1, 2, \dots, p \end{aligned}$$

Since this is true for all values of  $x_1, \dots, x_{n-1}$ ,

$$\begin{aligned} g_i(x_1, \dots, x_{n-1}) &= 0 \quad \text{for } i > p \\ &= f_i(x_1, \dots, x_{n-1}) \quad \text{for } i = 1, 2, \dots, p \end{aligned}$$

Thus, the uniqueness of the representation is established.

§3, ex. 11 (Used in §6, Ch. 11)

$$\begin{aligned}
 \text{Let } f(x, x_1, \dots, x_n) &\equiv \sum_{j=0}^m P_j(x_1, \dots, x_n)x^j. \text{ Then} \\
 f &\equiv f - 0 \equiv \sum_{j=0}^m P_j x^j - \sum_{j=0}^m P_j g_1^j - \sum_{j=1}^m P_j (x^j - g_1^j) \\
 &\equiv \sum_{j=1}^m P_j (x - g_1)(x^{j-1} + x^{j-2}g_1 + \dots + xg_1^{j-2} + g_1^{j-1}) \\
 &\equiv (x - g_1)f_1(x, x_1, \dots, x_n)
 \end{aligned}$$

Thus, the desired result holds for  $k = 1$ .

Assume it for  $k = r$ , and let  $k = r + 1$ . By the hypothesis of the induction,

$$f(x, x_1, \dots, x_n) \equiv (x - g_1) \cdots (x - g_r)g(x, x_1, \dots, x_n)$$

Therefore,

$$f(g_{r+1}, x_1, \dots, x_n) = (g_{r+1} - g_1) \cdots (g_{r+1} - g_r)g(g_{r+1}, x_1, \dots, x_n) \equiv 0$$

By hypothesis,  $g_{r+1} - g_i \neq 0$  ( $i = 1, 2, \dots, r$ ). Therefore (§3, Ch. 11),  $g(g_{r+1}, x_1, \dots, x_n) = 0$ . From the result for  $k = 1$ ,  $g(x, x_1, \dots, x_n) = (x - g_{r+1})h(x, x_1, \dots, x_n)$ .

Thus, the desired result is established for  $k = r + 1$ .

§3, ex. 12 (Used in §6, Ch. 14)

Since  $y - r$  is a factor,  $[a_0(r)x^n + \dots + a_n(r)][b_0(r)x^m + \dots + b_m(r)] = 0$  for every  $x$ . Hence, one of the two factors vanishes identically. Therefore,  $a_i(r) = 0$  for every  $i$  or  $b_j(r) = 0$  for every  $j$ . The desired result follows by the factor theorem.

§5, ex. 7 (Part (b) is used in §6, Ch. 11)

Part (a) is proved in §4, Ch. 3 (where it is shown that  $S_i = S'_i + r_{i+1}S'_{i-1}$ ). Part (b) follows from (a) by solving the equations for  $t_1, t_2, \dots, t_{n-1}$  in terms of  $S_1, S_2, \dots, S_{n-1}$ .

§6, ex. 1 (Part (b) is used in §7, Ch. 11)

(a) If  $x_1, \dots, x_n$  are the roots of  $x^n - a_1x^{n-1} + \dots + (-1)^na_n$ , then  $S_i(x_1, \dots, x_n) = (-1)^i[(-1)^{n-i}a_i] = a_i$ .

(b) Let  $a_1, \dots, a_n$  be any complex numbers. Choose  $x_1, \dots, x_n$  so that  $S_i(x_1, \dots, x_n) = a_i$  ( $i = 1, 2, \dots, n$ ). Letting  $x_1 = a_1$ ,



$\dots, x_n = a_n$  in  $g(S_1, \dots, S_n) \equiv 0$ , we obtain  $g(a_1, \dots, a_n) = 0$ . Hence,  $g(y_1, \dots, y_n) \equiv 0$ .

## CHAPTER 12

§3, ex. 8 (Used in §7 and ex. 7, §9, Ch. 12)

Since every term in the expansion of the determinant has as a factor exactly one element of this row (or column), if every element in the row (or column) is multiplied by  $\lambda$  then every term in the expansion is multiplied by  $\lambda$ .

§3, ex. 9 (Used in §7 and ex. 7, §9, Ch. 12)

The determinant on the left is

$$\begin{aligned} \Sigma \pm a_{1j_1} a_{2j_2} \cdots a_{i-1, j_{i-1}} (a_{i, j_i} + b_{i, j_i}) a_{i+1, j_{i+1}} \cdots a_{nj_n} \\ = \Sigma \pm a_{1j_1} a_{2j_2} \cdots a_{i-1, j_{i-1}} a_{i, j_i} a_{i+1, j_{i+1}} \cdots a_{nj_n} \\ + \Sigma \pm a_{1j_1} a_{2j_2} \cdots a_{i-1, j_{i-1}} b_{i, j_i} a_{i+1, j_{i+1}} \cdots a_{nj_n} \end{aligned}$$

The last two sums are the determinants on the right side of the desired equality

§7, ex. 10 (Used in §4, Ch. 13)

If in 
$$D = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

we replace  $a_{j_1}, a_{j_2}, \dots, a_{j_n}$  by  $a_{i_1}, a_{i_2}, \dots, a_{i_n}$  and expand the resulting determinant  $D_1$  according to row  $i$ , we obtain  $D_1 = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}$ , where  $A_{j1}, A_{j2}, \dots, A_{jn}$  are the cofactors of  $a_{j1}, a_{j2}, \dots, a_{jn}$  in  $D$ .

But  $D_1 = 0$  since rows  $i$  and  $j$  are the same

§9, ex. 7 (Used in §5, Ch. 13)

If the first matrix has rank  $l$ , the rank of the second is at least  $k$ , since any non-zero  $l$ -rowed minor of the first is a  $k$ -rowed minor of the second.

If a  $(k+1)$ -rowed minor of the second does not have elements of the last column, it is a  $(k+1)$ -rowed minor of the first and, therefore, is zero. Suppose it does have elements of the last column. For example, let it be

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21} & a_{22} & \cdots & a_{2k} & a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,1}x_1 + a_{k+1,2}x_2 + \cdots + a_{k+1,n}x_n \end{vmatrix}$$

We may express this (ex. 9, §3, Ch. 12) as

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{11} & x_1 \\ a_{21} & a_{22} & \cdots & a_{2k} & a_{21} & x_1 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,1} & x_1 \end{vmatrix} \\
 + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{12} & x_2 \\ a_{21} & a_{22} & \cdots & a_{2k} & a_{22} & x_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,2} & x_2 \end{vmatrix} \\
 \cdots + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{1n} & x_n \\ a_{21} & a_{22} & \cdots & a_{2k} & a_{2n} & x_n \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,n} & x_n \end{vmatrix}$$

From each of these  $n$  determinants we can factor out the  $x_i$  which appears in every element in the last column (ex. 8, §3, Ch. 12). We obtain the sum of

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} & a_{1i} \\ a_{21} & a_{22} & \cdots & a_{2k} & a_{2i} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{k+1,1} & a_{k+1,2} & \cdots & a_{k+1,k} & a_{k+1,i} \end{vmatrix} x_i$$

for  $i = 1, 2, \dots, n$ .

The first  $k$  of these vanish since they have two identical columns. The others are zero because they are  $(k+1)$ -rowed minors of the first matrix.

Thus, every  $(k+1)$ -rowed minor of the second matrix is zero. Hence, this matrix has rank  $k$ .

§9, ex. 9 (Used in §2, Ch. 13)

According to ex. 7, §9, Ch. 12, (working with rows instead of columns), the given matrix has the same rank as

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \cdots & \vdots \\ a_{m-1,1} & \cdots & a_{m-1,n} \end{pmatrix}$$

which is surely less than  $m$  since there are only  $m-1$  rows. Or, we can show directly that every  $m$ -rowed minor vanishes by proceeding as in ex. 7.

## CHAPTER 13

§7, ex. 5 (The first part is used in §3, Ch. 14)

If  $c_1 f_1(x) + \cdots + c_m f_m(x) \equiv 0$ , where the  $c_i$  are constants not all zero, multiplying both sides by  $g(x)$  establishes the desired result.

# NUMERICAL ANSWERS

## CHAPTER 1

*Sect. Ex.*

2— 8 12 and 14 fail

9 12 and 14 fail

3— 1 a)  $-117 + 44i$  c)  $6_5 + 12i/5$  e)  $2 - i$  g)  $-2i$

b)  $-i$  d)  $i$  f)  $6_{25}$

2 a)  $x = 1, y = -1$  d)  $x = -2, y = -1$

b)  $x = 1_4, y = -1$  e)  $x = 3_2, y = 0$

c)  $x = -3_2, y = -2$  f)  $x = 4_3, y = -1_6$

3 a)  $a = 2, b = 3$  c)  $a = 3_1, b = -1_4$  e)  $a = 1_1, b = 5_4$

b)  $a = 2, b = -3$  d)  $a = 7_{12}, b = 5_{12}$

13 a)  $\pm \frac{(1+i)}{\sqrt{2}}$  c)  $+(3+2i)$

b)  $\pm(2-i)$  d)  $\pm \frac{(7-i)}{\sqrt{2}}$

4 - 9 a) On circle of radius 1, center at origin

b) Inside or on circle of radius 1, center at (2, 0)

c) Points with abscissa  $3_4$

d) On real axis with non-negative abscissas

e) 1 and  $-1$

13 a)  $1_5$  c)  $1_{64}$  e) 2

b) 256 d)  $\sqrt{2}$  f) 1

5— 3 a)  $-\frac{i}{8}$  c)  $-1_4$  e)  $-\sqrt{3} + i$

b)  $128(-1 + i\sqrt{3})$  d)  $1$  f)  $-1$

6  $\cos 5\theta = \cos^5 \theta - 10 \cos^3 \theta \sin^2 \theta + 5 \cos \theta \sin^4 \theta$

$\sin 5\theta = 5 \cos^4 \theta \sin \theta - 10 \cos^2 \theta \sin^3 \theta + \sin^5 \theta$

6— 1 a)  $-3, \frac{3(1 \pm i\sqrt{3})}{2}$  d)  $-3, \frac{3(1 \pm \sqrt{3})}{2}$

b)  $\pm 2, \pm(1 \pm i\sqrt{3})$  e)  $\pm(\sqrt{3} + i)$

c)  $\pm \sqrt{2}(1 \pm i)$  f)  $\pm 1, \pm i, \pm \frac{(1+i)}{\sqrt{2}}$

## CHAPTER 2

4—19  $a_n = \frac{1}{6}[(\lambda - 16)n^3 + (102 - 6\lambda)n^2 + (11\lambda - 176)n + 96 - 6\lambda]$

20  $f(x) = \frac{1}{5}x^5 - \frac{1}{2}x^2 + \frac{1}{6}x$

$1^2 + \dots + n^2 = n(n+1)(2n+1)/6$

5— 1 a) No c) No e) Yes g) Yes i) No

b) No d) Yes f) No h) Yes j) No

## Sect. Ex.

6— 1 a)  $Q \equiv 2x - 1, R \equiv 0$

b)  $Q \equiv x^2 + 2x - 3, R \equiv -7$

c)  $Q \equiv x^2 - 3x + 8, R \equiv -27x + 7$

d)  $Q \equiv 2x^2 - 3x, R \equiv 1$

e)  $Q \equiv x^2 + 7x + 3, R \equiv 14x^2 - 18x - 14$

f)  $Q \equiv \frac{1}{2}(x^2 + x + 1), R \equiv 0$

g)  $Q \equiv 0, R \equiv 3x^2 - x - 1$

h)  $Q \equiv x + 1, R \equiv -x^3 - x^2 - x$

3 a) 10 b) 15 c)  $r$  d) 0 e)  $1 - r$  f)  $x^3 - 1$  g)  $r^{16}x^4 + 1$

5  $R \equiv 0$

6  $f(1) = -1, f(2) = 1$

7  $3(x + 3)$

9  $2x + 5$

10  $\frac{1}{2}(x^2 + 3x)$

7— 1 a) Yes b) Yes c) No d) Yes e) No

2 a)  $-1, -2$  b) 2,  $-4$  c) 3 d) 2,  $-1$  e) None f) All

3 a)  $k = 4, l = -1$  b)  $k = 0$ , any  $l$ ; or  $k = 1, l = 0$

9— 4 a)  $x + 1$  d) 1 g)  $2x + 3$

b)  $x^2 + x + 1$  c)  $x^2 + 2x + 3$  h) 1

c)  $x^3 - 2x + 1$  f)  $x^2 - 2$  i)  $4x^3 + 8x^2 - 3x - 9$

7  $a = 0$  or  $1, b = 0$

8  $r = 2$

13  $f$  denotes the first of the given polynomials,  $g$  the second

a)  $2(x + 1) - (x + 1)f - (x^2 + 4x + 4)g$

b)  $x^2 + x + 1 \equiv (x - 1)f - (x^2 + 2)g$

c)  $5(x^3 - 2x + 1) - 4f - (2x + 3)g$

d)  $56 \equiv (6x^3 + 3x^2 - 19x - 21)f - (2x^2 + x^2 - 9x - 7)g$

e)  $23(x^2 + 2x + 3) \equiv -3(2x + 3)f + 4g$

f)  $2(x^2 - 2) \equiv -f + (x - 1)g$

g)  $560(2x + 3) \equiv (9x - 22)f - (15x + 37)g$

h)  $1008 \equiv (x^2 - 8x - 35)f - (x^2 - 14x + 31)g$

i)  $3(4x^3 + 5x^2 - 3x - 9) \equiv -f + (2x + 1)g$

10— 1 a) Relatively prime d) Relatively prime

b) Relatively prime e) H.C.F.  $x^2 - 2$

c) H.C.F.  $x^2 - x + 1$  f) Relatively prime

11— 1 a)  $(x^2 + 1)(x^2 + 3)$  d)  $(x^2 - 1 + \sqrt{2})(x^2 - 1 - \sqrt{2})$

b)  $(x^2 + i)(x^2 - i)$  e)  $(x + \frac{1}{2} + \frac{1}{2}\sqrt{5})(x + \frac{1}{2} - \frac{1}{2}\sqrt{5})$

c)  $(x - 1)(x^2 + x - 1)$  f)  $(2x - 1)(x^2 + x + 1)$

12— 1 a)  $(x^2 - 3)(x^2 - 2)$

b)  $(x + \sqrt{3})(x - \sqrt{3})(x + \sqrt{2})(x - \sqrt{2})$

c)  $(x + \sqrt{2})(x - \sqrt{2})(x^2 - 3)$

d)  $(x + \sqrt{3})(x - \sqrt{3})(x + \sqrt{2})(x - \sqrt{2})$

Sect. Ex.

- e)  $(x-1)^2(x^2+x+1)^2$   
 f)  $(x-1)^2(x^2+x+1)^2$   
 g)  $(x-1)^2\left(x+\frac{1+i\sqrt{3}}{2}\right)^2\left(x+\frac{1-i\sqrt{3}}{2}\right)^2$   
 h)  $(x+1)(x^2+1)$   
 i)  $(x+1)(x^2+1)$   
 j)  $(x+1)(x+i)(x-i)$   
 k)  $x^4+5x^2+2$   
 l)  $\left(x^2+\frac{5+\sqrt{17}}{2}\right)\left(x^2+\frac{5-\sqrt{17}}{2}\right)$

## CHAPTER 3

- 3— 1 a) Triple,  $(x-2)^3(x+5)$   
 b) Double,  $9(x-2)^2(x+i)(x-i)$   
 c) Triple,  $8(x+\frac{1}{2})^3(x+i)(x-i)$   
 d) Not a root  
 e) Double,  $(x+i)^2[4x^4+(4-8i)x^3-(3+5i)x^2-(4+2i)x-1]$   
 2 a)  $x^5-6x^4+12x^3-5x^2-0$   
 b)  $x^5-(1+4i)x^4+(4i-5)x^3+(5+2i)x^2-2ix=0$   
 c)  $x^4-4x^3+24x^2-40x+100=0$   
 d)  $x^3+(\sqrt{3}-3)x^2-2\sqrt{3}x+2-2\sqrt{3}=0$   
 e)  $4x^4-4x^3-x^2+x=0$   
 11  $a=1$ ; roots  $1, 1, \frac{1}{2}(1 \pm i\sqrt{7})$   
 12 If  $-2$  is a root then  $a=4$  and roots are  $-2, 2, -1$   
 13  $a=0$ , multiplicity 4,  $a=\pm 1$ , multiplicity 2  
 15  $a=-16, b=-3$   
 16  $a=b=-1$   
 4— 1 a)  $a=9; r=2, \pm 3i$   
 b) Either  $a=12; r=1, 2, -3$  or  $a=-12; r=-1, -2, 3$   
 c)  $a=2; r=-1, -1 \pm i$   
 d)  $a=-2; r=\frac{1}{6}, \frac{1}{3}, \frac{2}{3}$   
 e)  $a=-11; b=-6i; r=-i, -2i, -3i$   
 f) Either  $a=-108; r=-3, -9, 4$  or  $a=19404; r=\frac{1}{3}, \frac{2}{3}, \frac{1}{13}, \frac{2}{13}, \frac{1}{132}, \frac{2}{132}$   
 g)  $a=2; b=1; r=1 \pm \sqrt{2}, 1 \pm \sqrt{2}$   
 h)  $a=-4; b=5; r=\pm i, 2 \pm i$   
 i) Either  $a=2; r=\pm i, -1 \pm \sqrt{2}$  or  $a=-2; r=-1, -1, -1, 1$   
 j) Either  $a=b=c=0; r=0, 0, 0, -2, -2$  or  $a=-3^2\frac{1}{25}; b=-25\frac{9}{125}; c=2048\frac{8}{3125}; r=-\frac{8}{5}, -\frac{8}{5}, -\frac{8}{5}, \frac{3}{5}, \frac{3}{5}$

## Sect. Ex.

- k) Either  $a = 2; b = 16; r = 1 \pm i, 2 \pm 2i$  or  $a = -2; b = 16; r = -1 \pm i, -2 \pm 2i$  or  $a = 0; b = 129\frac{1}{2}; r = \pm i\sqrt{18\frac{1}{2}}, \pm 2i\sqrt{18\frac{1}{2}}$
- l)  $a = -\frac{3}{2}; b = 6; r = 2, \frac{1}{2}$
- m) Either  $a = 3; b = 1; r = -1, -1, -1$  or  $a = -21; b = 9, r = 3, -3 \pm 2\sqrt{3}$  or  $a = b = 0; r = 0, 0, -3$
- n)  $a = 0; r = 0, 0, 0$
- o) Either  $a = b = c = 0; r = 0, 0, 0$  or  $a = -3; b = 3; c = -1; r = 1, 1, 1$  or  $a = 1; b = c = -1; r = 1, -1, -1$
- 2 a)  $c(2b - a^2)$  d)  $3c - ab$  g)  $-2a + 4b - ab + 3c$   
 b)  $-b/c$  e)  $ab/c - 3$  h)  $3ab - a^3 - 3c$   
 c)  $-1 - a - b - c$  f)  $(b^2 - 2ac)/c^2$
- 7  $n > 2, a = b = 0$  or  $n = 2, b = a^2$
- 8 21
- 5—1 a)  $x^3 + 3ax^2 + 9bx + 27c = 0$   
 b)  $x^3 - ax^2 + bx - c = 0$   
 c)  $x^3 - bx^2 + acx - c^2 = 0$   
 d)  $x^3 + (2b - a^2)x^2 + (b^2 - 2ac)x - c^2 = 0$   
 e)  $c^2x^3 - acx^2 + bx - 1 = 0$   
 f)  $x^3 + (a - 6)x^2 + (b - 4a + 12)x + (4a - 2b + c - 8) = 0$   
 g)  $cx^3 + (6c + 2b)x^2 + (12c + 8b + 4a)x + (8c + 8b + 8a + 8) = 0$   
 h)  $(1 - a + b - c)x^4 + (3 - a - b + 3c)x^2 + (3 + a - b - 3c)x + (1 + a + b + c) = 0$   
 i)  $cx^3 + (b^2 - 2ac)x^2 + (a^2 - 2b)x + c^2 = 0$   
 j)  $x^3 + 2ax^2 + (a^2 + b)x + ab - c = 0$   
 k)  $x^3 + ax^2 + (4b - a^2)x + (4ab - a^3 - 8c) = 0$   
 l)  $x^6 + ax^4 + bx^2 + c = 0$
- 2 a)  $x^3 + 3x^2 - 3x - 5 = 0$  d)  $2x^4 - 2x^3 - 3x^2 - 4x = 0$   
 b)  $3x^4 - x^3 + 7x + 4 = 0$  e)  $3x^5 + 3x^2 + 2 = 0$   
 c)  $4x^6 - 2x^5 - x^2 - x - 1 = 0$
- 3 a)  $5x^3 - 3x^2 - 3x + 1 = 0$  d) None  
 b)  $4x^4 - 7x^3 + x + 3 = 0$  e)  $2x^5 + 3x^3 - 3 = 0$   
 c)  $x^6 - x^5 + x^4 - 2x - 4 = 0$
- 4 a)  $k = -2, x^3 + 6x^2 - 12x - 40 = 0; k = \frac{1}{3}, 27x^3 - 27x^2 - 9x + 5 = 0; k = i, x^3 - 3ix^2 + 3x - 5i = 0$   
 b)  $k = -2, 3x^4 - 2x^3 + 56x + 64 = 0; k = \frac{1}{3}, 243x^4 + 27x^3 - 21x + 4 = 0; k = i, 3x^4 + ix^3 + 7ix + 4 = 0$   
 c)  $k = -2, 4x^6 - 4x^5 - 16x^3 - 32x - 64 = 0; k = \frac{1}{3}, 2916x^6 + 486x^5 - 9x^3 + 3x - 1 = 0; k = i, 4x^6 + 2ix^5 - x^2 + ix + 1 = 0$   
 d)  $k = -2, x^4 - 2x^3 - 6x^2 - 16x = 0; k = \frac{1}{3}, 54x^4 + 18x^3 - 9x^2 + 4x = 0; k = i, 2x^4 + 2ix^3 + 3x^2 - 4ix = 0$

Sect. Ex.

- e)  $k = -2$ ,  $3x^5 + 24x^2 + 64 = 0$ ;  $k = \frac{1}{3}$ ,  $729x^5 - 27x^2 - 2 = 0$ ;  
 $k = i$ ,  $3x^5 + 3ix^2 - 2i = 0$
- 5 a) 1                      b) 3                      c) 4                      d) 2                      e) 3
- 8  $27x^3 + (27b - 9a^2)x + (27c - 9ab + 2a^3) = 0$
- 6—2 a) -1                      d) None                      g)  $-\frac{3}{2}$   
 b)  $\frac{1}{2}(-1 \pm i\sqrt{3})$                       e)  $-1 \pm i\sqrt{2}$                       h) None  
 c)  $1, \frac{1}{2}(-1 \pm \sqrt{5})$                       f)  $\pm\sqrt{2}$                       i)  $1, -\frac{3}{2}, -\frac{3}{2}$
- 3 a)  $\pm\frac{1}{2}$                       c)  $-1, -\frac{2}{3}$                       e)  $\frac{1}{2}(-1 \pm i\sqrt{3})$   
 b)  $\pm i$                       d)  $\frac{1}{2}, \frac{3}{2}$
- 4 a)  $4, \frac{1}{2}$                       c)  $\frac{1}{2}, 2$                       e) 0                      g) None  
 b)  $0, 1, -9$                       d)  $0, -1, 9$                       f) All  $k$
- 6 a)  $a$  arbitrary,  $b = 0$                       c) All values of  $a, b$   
 b)  $a$  arbitrary,  $b = 0$
- 7 The common root is  $a$ , which is multiple

CHAPTER 4

- 1—14  $a$  and  $b$  are arbitrary constants
- a)  $ax + b$                       c)  $a(x^2 - 1)$                       e)  $x^3 + ax^2 + b(2x - 1)$   
 b)  $ax^2 - x + 1$                       d)  $a(x^2 - 1) + bx$
- 2—1 a) -2 triple,  $3 + i\sqrt{15}$  simple  
 b) No multiple roots  
 c)  $1 + i$  double,  $1 + \sqrt{2}$  simple  
 d) 3 double;  $-1, 4$  simple  
 e) No multiple roots  
 f)  $-1 - i$  double,  $2 + 2i$  simple  
 g)  $(3 \pm i\sqrt{15})/6$  double,  $(-3 \pm i\sqrt{6})/3$  simple  
 h) No multiple roots  
 i) 1 fourfold,  $-2 + \sqrt{3}$  simple
- 2 a)  $-1, 2 \pm 2i\sqrt{3}$                       z) All values  
 b) 0, 2                      h) 0  
 c)  $0, +2i\sqrt{3}/9$                       i)  $0, -1, (1 \pm i\sqrt{3})/8$   
 d)  $0, \frac{1}{4}$                       j) No values  
 e) 0, 1                      k)  $0, 1, (-1 \pm i\sqrt{3})/2$   
 f) All values
- 12 b)  $n = 3$
- 15  $n = 4$ ,  $a = -1/2$ ,  $b = 2$
- 16 If  $n$  is even,  $a = 0, -1/2$ ; if  $n$  is odd,  $a = 0, \pm 1/2$
- 18 Either  $a = 0$  or  $n = 3$ ,  $a = -2$
- 4—1 a)  $10 - 15(x + 1) + 13(x + 1)^2 - 8(x + 1)^3 + 2(x + 1)^4$   
 b)  $-54(x - 3)^2 + (x - 3)^4$   
 c)  $18i + 2 + (x - 2i) + 6i(x - 2i)^2 + (x - 2i)^3$   
 d)  $(x - 1 + 2i)^4$   
 e)  $-\frac{3}{2} - 3(x - \frac{1}{2}) + 9(x - \frac{1}{2})^3$

## Sect. Ex.

- 2 a)  $c_0 = 0, c_1 = 1, c_2 = -3, c_3 = 1$   
 b)  $c_0 = -2, c_1 = 3, c_2 = 4, c_3 = 1$   
 c)  $c_0 = -2, c_1 = -2, c_2 = 3, c_3 = -2, c_4 = 1$   
 d)  $c_0 = 1, c_1 = -2, c_2 = 3, c_3 = -1, c_4 = 1$   
 e)  $c_0 = -i, c_1 = 1, c_2 = i - 2, c_3 = -1, c_4 = 1$   
 4 a)  $x^4 + 11x^3 + 47x^2 + 93x + 73 = 0$   
 b)  $x^4 - 5x^3 + 11x^2 - 11x + 5 = 0$   
 c)  $2x^3 - 25x^2 + 102x - 133 = 0$   
 d)  $2x^3 + 11x^2 + 18x + 11 = 0$   
 e)  $x^4 + (4i - 2)x^3 - (3 + 6i)x^2 + (2i + 4)x = 0$   
 f)  $2x^4 - 16x^3 + 45x^2 - 45x + 5 = 0$   
 6  $-76g''' + g'' + g' + 6g$

## CHAPTER 5

- 1— 3 a)  $-2, -2, \pm 2i$  c)  $1 \pm i, 1 + i, \pm i$  e)  $i, 1 \pm \sqrt{3}$   
 b)  $\pm i, \pm \sqrt{5}, \frac{1}{2}(1 \pm i)$  d)  $1, -1, 1 \pm i, \pm i$   
 4 a)  $x^4 - 8x^3 + 26x^2 - 40x + 25$   
 b)  $x^6 - 2x^5 + 4x^4 - 4x^3 + 5x^2 - 2x + 2$   
 c)  $x^6 + 3x^4 + 3x^2 + 1$   
 d)  $x^4 - 6x^3 + 14x^2 - 16x + 8$   
 e)  $x^4 - 4x^3 + 11x^2 - 14x + 12$   
 5 a)  $a = +3, k = -18$  e)  $a = 0, k = 0$   
 b)  $a = +1, k = 0$  f)  $a = 8, k = -8$   
 c)  $a = 0, k = 0$  g)  $a = 1, k = 9$   
 d)  $a = -2, k = -39$  or  
 $a = \frac{1}{2}, k = 106\frac{1}{2}$   
 2— 1 a)  $\frac{1}{3}, -\frac{1}{3}, \frac{1}{2}(-1 \pm i\sqrt{3})$  f)  $-\frac{2}{3}, -\frac{2}{3}, \pm i\sqrt{2}, \pm i\sqrt{2}$   
 b) No rational roots g)  $-\frac{1}{2}, -\frac{1}{2}, \pm i, \pm i$   
 c)  $\frac{2}{3}, \frac{2}{3}, \pm i$  h)  $2, \frac{3}{2}, \pm 2i$   
 d)  $-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \pm i$  i)  $\frac{1}{2}, \frac{1}{2}, \pm 3i$   
 e) No rational roots  
 3 a)  $k = 3, x = -2$  g)  $k = 1, x = \frac{1}{2};$   
 b)  $k = 2, x = -1, -2, 3;$   $k = 3, x = 1;$   
 $k = -2, x = 1, -2, -3;$   $k = -5, x = -1$   
 All other values of  $k, x = -2$   $k = -9, x = -\frac{1}{2}$   
 c)  $k = 2, x = -1, -1, 3, 3$  h)  $k = 0, x = 0;$   
 d) None  $k = 1, x = 1;$   
 e)  $k = 1, x = 0$   $k = -5, x = \frac{5}{2}$   
 f)  $k = -n^2$  ( $n$  any integer),  $x = -1, n,$  i)  $k = 1, x = 1;$   
 $-n$ ; all other values of  $k, x = -1$   $k = 10, x = -\frac{1}{2}$   
 $k = 15, x = -\frac{1}{2}$   
 j) No values of  $k$



## Sect. Ex.

- 6 a)  $a = b = -1, x = 1, 1, -1$   
 b)  $a = -6, b = -8, x = -1, -1, -1, 3$ ; or  $a = -6, b = 8, x = 1, 1, 1, -3$   
 c)  $a = -5, b = 7, x = 1, 1, 3$ ; or  $a = 3, b = -1, x = 1, -1, -3$ ; or  $a = -1, b = -5, x = -1, -1, 3$
- 7 a)  $a = -2, b = 4, c = 9, x = -1, -1, -1, \frac{1}{2}(3 \pm i\sqrt{7})$   
 b)  $a = -8, b = 18, c = -16, x = 1, 1, 1, 5$ ; or  $a = 4, b = -6, c = -4, x = 1, 1, -1, -5$ ; or  $a = 8, b = 18, c = 16, x = -1, -1, -1, -5$ ; or  $a = -4, b = -6, c = 4, x = -1, -1, 1, 5$
- 3--1 a)  $1 + \sqrt{5}, \frac{1}{4}(-3 \pm i\sqrt{7})$   
 b)  $1 \pm \sqrt{2}, 1 \pm \sqrt{2}, \pm i\sqrt{2}$   
 c)  $2 \pm \sqrt{3}, 3 \pm \sqrt{2}, \frac{1}{2}(-3 \pm i\sqrt{3})$   
 d)  $2 \pm \sqrt{2}, \pm \frac{(1 + i\sqrt{3})}{\sqrt{2}}$   
 e)  $\pm \sqrt{3}, 3 \pm \sqrt{2}, \pm i\sqrt{2}, -1$
- 2 a)  $x^4 - 12x^3 + 40x^2 - 24x + 4$   
 b)  $x^6 - 14x^5 + 40x^4 + 54x^3 - 276x^2 - 126x + 414$   
 c)  $x^6 - 6x^4 + 12x^2 - 8$   
 d)  $x^4 - 12x^2 + 16$   
 e)  $x^4 - 8x^3 + 12x^2 + 4x - 1$
- 4 a)  $\pm 2\sqrt{2} \pm \sqrt{3}, 1$   
 b)  $\pm \sqrt{14} \pm \sqrt{7}, \pm i\sqrt{42}$   
 c)  $\pm \sqrt{6} \pm \sqrt{12}, \frac{1}{2}(-1 \pm i\sqrt{3})$   
 d)  $\pm \sqrt{5} + i\sqrt{6}, -1, \frac{1}{2}(1 \pm \sqrt{5})$   
 e)  $\pm \sqrt{2}, \sqrt{3}, \frac{1}{2}$
- 5 a)  $x^4 - 14x^2 + 9$  d)  $x^6 - 33x^4 - 25x^2 + 9$   
 b)  $x^4 - 60x^2 + 36$  e)  $x^4 + 20x^2 + 196$   
 c)  $x^5 - x^4 - 22x^3 + 22x^2 + x - 1$
- 6 a)  $a = -3, b = -10, x = -1, 1 \pm \sqrt{5}$   
 b)  $a = -20, b = 3, x = 2, 3 \pm 2\sqrt{3}$   
 c)  $a = 0, b = -2, x = 0, \pm \sqrt{2}$ , or  $a = 2, b = 10, x = 2, 2 + \sqrt{2}$ ; or  $a = -2, b = 10, x = -2, -2 \pm \sqrt{2}$   
 d)  $a = -4, b = -1, x = \pm i, 2 \pm \sqrt{5}$   
 e)  $a = \pm 3, b = -357, x = 1 + 3\sqrt{2}, -1 \pm 2i\sqrt{5}$
- 7 a)  $a = 3, b = 24, x = 3 \pm \sqrt{3}, -2$   
 b)  $a = -19, b = -109, x = -9, 1 \pm 4i/3$   
 c)  $a = -6, b = -252, x = 6, -6 \pm i\sqrt{6}$   
 d)  $a = 7, b = 2, x = -1, 7, 2 \pm \sqrt{7}$
- 9  $a = -2, b = 0, x = 1, \frac{1}{2}(1 \pm \sqrt{5})$ ; or  $a = b = 0, x = -1, \frac{1}{2}(1 \pm i\sqrt{3})$
- 10  $a = -2, x = 2, -1 \pm i$

## Sect. Ex.

12  $a = 0, b = -8, c = -1, d = 3$

13  $a = -2, b = 6, c = 5, d = 1, e = 2$

- 7— 1 a)  $x \leq 0, x \geq 4$  increasing;  $0 \leq x \leq 4$  decreasing  
 b)  $x \leq 0$  decreasing;  $x \geq 0$  increasing  
 c)  $x \leq 3$  decreasing;  $x \geq 3$  increasing  
 d)  $x \leq -2, x \geq 5$  increasing;  $-2 \leq x \leq 5$  decreasing  
 e)  $x \leq -1, 0 \leq x \leq 1$  decreasing;  $-1 \leq x \leq 0, x \geq 1$  increasing  
 f)  $x \leq 0, x \geq 3$  increasing;  $0 \leq x \leq 3$  decreasing  
 g) Always increasing  
 h)  $x \leq 0, x \geq 4$  increasing;  $0 \leq x \leq 4$  decreasing  
 i)  $x \leq 5$  decreasing;  $x \geq 5$  increasing  
 j)  $x \leq -1, x \geq \frac{1}{2}$  increasing;  $-1 \leq x \leq \frac{1}{2}$  decreasing

## CHAPTER 6

- 4— 2 a) One in  $[-1, 0]$ ; one in  $[2, 3]$   
 b) None in  $[1, 2]$ ; one in  $[0, 1]$   
 c) None or two in  $[-1, 0]$ ; one in  $[0, 1]$   
 d) None or two in  $[0, 1]$ ; none in  $[-2, -1]$   
 e) None in  $[-3, -1]$ , none or two in  $[-1, 0]$   
 f) None in  $[-1, 0]$ , two in  $[1, 2]$  if  $n = 3$ , none or two if  $4 \leq n \leq 7$ , none if  $n \geq 8$   
 g) One  
 3 None if  $a \geq 0$ , one if  $a \leq -2$ ; none or two if  $-2 < a < 0$   
 4 One if  $-7a^3 < b < a^3$ , otherwise none  
 5— 2 a) One greater than 2; one or three greater than  $-3$  (compare ex. 3(e), §5)  
 b) None greater than 1; none or two greater than  $-2$  (compare ex. 3(d), §8)  
 c) None less than  $-2$ , one less than 1  
 d) One less than  $\frac{1}{2}$ , none less than 0  
 e) None greater than 2; none less than  $-2$   
 f) One  
 g) One  
 h) One if  $-\frac{3}{4} \leq a \leq 0$ ; one or three if  $a < -\frac{3}{4}$  (compare ex. 3(f), §8)  
 i) None  
 3 a) No positives, no negatives  
 b) One positive, one negative  
 c) One positive, no negatives  
 d) One positive, one negative  
 e) Two positives, one negative  
 f) One positive, two negatives

**Sect. Ex.**

- g) One positive, no negatives
- h) One or three positives, one negative (compare ex. 1(g), §8)
- i) Two or no positives, no negatives (compare ex. 1(d), §8)
- j) One positive, one negative
- k) No positives, no negatives if  $b = 0$ ; no positives, one negative if  $b > 0$ ; one positive, no negatives if  $b < 0$
- l) One positive, one negative if  $n$  is even; one positive, no negatives if  $n$  is odd

- 7— 1**
- a) None in  $[0, 1]$  or  $[1, 2]$
  - b) None in  $[1, 2]$ ; one in  $[3, 4]$
  - c) None in  $[-1, 1]$ ; none in  $[-5, 5]$
  - d) None in  $[0, 3]$ ; one in  $[-2, 0]$
  - e) One in  $[-2, 0]$ ; none in  $[0, 1]$
  - f) One in  $[-1, 0]$ ; one in  $[-3, -1]$
  - g) One in  $[1, 2]$ ; none in  $[-1, 0]$
  - h) Two in  $[0, 1]$ ; three in  $[-8, 0]$
  - i) None in  $[0, 1]$ ; two in  $[-2, 0]$
  - j) One in  $[-4, -3]$ , none in  $[1, 2]$
  - k) None in  $[-1, 0]$ ; one in  $[0, 1]$
  - l) None in  $[-1, 0]$ ; none in  $[-3, -1]$

- 8— 1**
- a) One positive, no negatives
  - b) No positives, no negatives
  - c) One positive, one negative
  - d) No positives, no negatives
  - e) One positive, two negatives
  - f) One positive, one negative
  - g) One positive, one negative
  - h) No positives, one negative
  - i) One positive, one negative
  - j) One positive, no negatives
  - k) One positive, one negative
  - l) One positive, no negatives
- 2**
- a) Two in  $[-1, 0]$ , one in  $[2, 3]$
  - b) One in  $[2, 3]$
  - c) One in  $[1, 2]$ , one in  $[-4, -3]$ , one in  $[-2, -1]$
  - d) One in  $[-4, -3]$
  - e) One in  $[-4, -3]$ , one in  $[2, 3]$
  - f) One in  $[-4, -3]$ , one in  $[-2, -1]$
  - g) One in  $[1, 2]$
  - h) One in  $[0, 1]$ , one in  $[4, 5]$
- 4**
- a) Six if  $a = 0$ , none if  $a > 0$ , two if  $a < 0$
  - b) Six if  $a = 0$ , none if  $a > 0$ , two if  $a < 0$

## Sect. Ex.

- c) One if  $a \geq 0$ , three if  $-1 \leq a < 0$ , one if  $a < -1$   
 d) None if  $a > 0$ , two if  $a \leq 0$   
 e) None if  $a \geq 0$ , two if  $a < 0$

## CHAPTER 7

The first three decimal places are given.

- 2 a) 1.577, 5.656, -1.233 e)  $\pm 1.224$ ,  $\pm 0.629$  i) 4.000, 5.641  
 b) 1 000, -0.333 f) 5.493 j) -1.280  
 c) 0.669, 3.984 g) -0.991  
 d) 9.463, -1.363, -2.600 h) 4.000, -2.423
- 5— 1 a) -0.538 e) 1.154 i) 1.565  
 b) -2.534 f) 2.344 j) -0.183  
 c) -2.185 g) 1.915  
 d) 1.587 h) 0.433
- 2 a) -0.500, 2.414, -0.414 e) 2.114, -3 101  
 b) 2 930 f) -1 899, -3.407  
 c) 1 330, -1.201, -3.128 g) 1.167  
 d) -3.900 h) 0.707, 4.174
- 3 See §2
- 7— 2 4.718  
 3 1.839  
 4 3 569  
 5 2.359  
 6 1.783  
 7 1.912  
 8 1.732  
 9 2.094  
 10 -4.848

## CHAPTER 8

- 4— 1 a)  $x = z - \frac{2}{z} - 1$ ;  $z = \sqrt[3]{4}, \omega \sqrt[3]{4}, \omega^2 \sqrt[3]{4}$   
 b)  $x = z - \frac{4}{z} + 2$ ;  $z = 2 \sqrt[3]{2}, 2\omega \sqrt[3]{2}, 2\omega^2 \sqrt[3]{2}$   
 c)  $x = z + \frac{1}{z}$ ;  $z = -1, -\omega, -\omega^2$   
 d)  $x = z - \frac{2a^2}{z}$ ;  $z = -a \sqrt[3]{2}, -\omega a \sqrt[3]{2}, -\omega^2 a \sqrt[3]{2}$   
 e)  $x = z + \frac{2}{z} - 1$ ;  $z = \alpha, \alpha\omega, \alpha\omega^2$ ;  $\alpha = \frac{\sqrt[3]{2}(\sqrt{3} + i)}{2}$   
 f)  $x = z - \frac{i}{z}$ ;  $z = -1, -\omega, -\omega^2$

**Sect. Ex.**

$$g) y = z + \frac{\sqrt[3]{4}}{z}; z = -\sqrt[3]{2}, -\omega\sqrt[3]{2}, -\omega^2\sqrt[3]{2}$$

$$h) y = z - \frac{2i}{z}; z = 1, \omega, \omega^2$$

$$i) y = z - \frac{2\omega}{z}; z = -i, -\omega i, -\omega^2 i$$

$$j) x = z - \frac{4}{z}; z = 2\sqrt[3]{2}, 2\omega\sqrt[3]{2}, 2\omega^2\sqrt[3]{2}$$

$$k) x = z - \frac{6}{z}; z = \sqrt[3]{12}, \omega\sqrt[3]{12}, \omega^2\sqrt[3]{12}$$

$$l) x = z + \frac{i}{z}; z = -1, -\omega, -\omega^2$$

$$m) y = z + \frac{4\omega}{z}; z = 2, 2\omega, 2\omega^2$$

$$n) x = z + \frac{9}{z}; z = 3, 3\omega, 3\omega^2$$

$$o) x = z - \frac{2}{z}; z = 1 + i, \omega(1 + i), \omega^2(1 + i)$$

5— 1 a) One real, two imaginary      d) One real, two imaginary

b) One real, two imaginary      e) Three real

c) Three real

2 a) Three real if  $-2 \leq a \leq 2$ , otherwise one real

b) Three real if  $a \leq -3$ , otherwise one real

c) Three real if  $0 < a \leq \frac{1}{4}$ , otherwise one real

d) Three real if  $a = 0$ , otherwise one real

e) Three real if  $a \leq \sqrt[3]{-4}$ , otherwise one real

f) Three real if  $a \leq 0$ , otherwise one real

3 a)  $\pm 54$       c) All      e) None      g) All

b)  $0, \pm 18$       d)  $3 \pm 2\sqrt{3}$       f)  $0, \pm i$

6 a)  $4\sqrt{3} \cos 10^\circ, 4\sqrt{3} \cos 130^\circ, 4\sqrt{3} \cos 250^\circ$

b)  $2\sqrt{2} \cos 45^\circ, 2\sqrt{2} \cos 165^\circ, 2\sqrt{2} \cos 285^\circ$

c)  $2 \cos 40^\circ, 2 \cos 160^\circ, 2 \cos 280^\circ$

d)  $4 \cos 46^\circ 11' 48'', 4 \cos 166^\circ 11' 48'', 4 \cos 286^\circ 11' 48''$

e)  $2\sqrt{2} \cos 23^\circ 5' 54'', 2\sqrt{2} \cos 143^\circ 5' 54'', 2\sqrt{2} \cos 263^\circ 5' 54''$

f)  $2\sqrt{2} \cos 15^\circ - 1, 2\sqrt{2} \cos 135^\circ - 1, 2\sqrt{2} \cos 255^\circ - 1$

7— 1 a)  $\frac{1}{2}(-\sqrt{5} \pm 1), \frac{1}{2}(-\sqrt{5} \pm 3)$

b)  $\frac{1}{2}(-1 \pm \sqrt{5}), \frac{1}{2}(1 \pm i\sqrt{7})$

c)  $-3, -3, 1 \pm i\sqrt{2}$

d)  $-1 \pm \sqrt{3}, 1 \pm \sqrt{2}$

e)  $\frac{1}{2}(-3 \pm \sqrt{5}), \frac{1}{2}(1 \pm i\sqrt{3})$

## Sect. Ex.

- f)  $\frac{1}{2}(-1 \pm \sqrt{13})$ ,  $\frac{1}{2}(3 \pm \sqrt{5})$   
 g)  $\frac{1}{2}(1 \pm i\sqrt{15})$ ,  $\frac{1}{2}(3 \pm \sqrt{13})$   
 h)  $\frac{1}{2}(-i \pm \sqrt{3})$ ,  $\frac{1}{2}(1 \pm \sqrt{5})i$   
 i)  $i \pm \sqrt{3}$ ,  $-i \pm i\sqrt{3}$   
 j)  $1, 3, \pm i$   
 k)  $\frac{1}{2}(-1 \pm i\sqrt{11})$ ,  $\frac{1}{2}(-1 \pm \sqrt{13})$   
 l)  $\frac{1}{2}(-1 \pm \sqrt{5})$ ,  $\frac{1}{2}(1 \pm i\sqrt{11})$   
 m)  $\frac{1}{2}(-3 \pm \sqrt{5})$ ,  $\frac{1}{2}(-1 \pm i\sqrt{11})$   
 n)  $\frac{1}{2}(-3 \pm i\sqrt{11})$ ,  $\frac{1}{2}(3 \pm i\sqrt{7})$   
 o)  $2 \pm i\sqrt{5}$ ,  $-2 \pm i\sqrt{3}$   
 p)  $-1 \pm i$ ,  $1 \pm i\sqrt{2}$   
 q)  $\frac{1}{2}(-1 - \sqrt{3} \pm i\sqrt[4]{12})$ ,  $\frac{1}{2}(-1 + \sqrt{3} \pm i\sqrt[4]{12})$   
 r)  $\frac{1}{2}(1 - i)(1 \pm \sqrt[4]{13})$ ,  $\frac{1}{2}(1 - i)(-1 \pm \sqrt[4]{13})$   
 s)  $\pm \frac{1}{2}$ ,  $\frac{1}{4}(1 \pm \sqrt{5})$   
 t)  $-\sqrt[3]{2}$ ,  $-\sqrt[3]{2}$ ,  $(\sqrt{2} \pm 2i)/(2\sqrt{3})$   
 u)  $\frac{1}{2}(-\sqrt{6} \pm \sqrt{4\sqrt{6}-6})$ ,  $\frac{1}{2}(\sqrt{6} \pm i\sqrt{4\sqrt{6}+6})$   
 v)  $\frac{1}{2}(-2 - \sqrt{2} \pm \sqrt{8\sqrt{2}+10})$ ,  
 $\frac{1}{2}(-2 + \sqrt{2} \pm i\sqrt{8\sqrt{2}-10})$   
 w)  $\frac{1}{2}(-2 - \sqrt{3} \pm i\sqrt{4\sqrt{3}+9})$ ,  
 $\frac{1}{2}(-2 + \sqrt{3} \pm i\sqrt{9-4\sqrt{3}})$

## CHAPTER 10

- 5— 6 a)  $a + bi$ ;  $a, b$  any real numbers  
 b)  $a + b\sqrt{2}$ ;  $a, b$  any rational numbers  
 c)  $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ ;  $a, b, c, d$  any rational numbers  
 d)  $a + b\sqrt{7}$ ;  $a, b$  any rational numbers  
 e)  $a + bi$ ;  $a, b$  any real numbers  
 f)  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ ;  $a, b, c$  any rational numbers  
 g)  $a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\sqrt{2} + e\sqrt{2}\sqrt[3]{2} + f\sqrt{2}\sqrt[3]{4}$ ;  $a, b, c, d, e, f$  any rational numbers  
 h)  $a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\sqrt{5} + e\sqrt{5}\sqrt[3]{2} + f\sqrt{5}\sqrt[3]{4}$ ;  $a, b, c, d, e, f$  any rational numbers  
 7  $1 + 4\xi + 4\xi^2$ ;  $-1 - \frac{1}{2}\xi^2$ ;  $5 - 2\xi + 2\xi^2$   
 8  $9 + \xi - 3\xi^2$ ;  $26\xi + 9$

CHAPTER 11

Sect. Ex.

- 7— 1 a)  $S_2^2 - 2S_1S_3$  g)  $S_1^4 - 4S_1^2S_2 + 2S_2^2 + 4S_1S_3$   
 b)  $S_3^2 - 2S_2S_4$  h)  $3S_1^2 + S_2$   
 c)  $S_2S_4$  i)  $S_1^2S_4 - 4S_2S_4 + S_3^2$   
 d)  $S_2S_3$  j)  $-S_1^3 + 4S_1S_2 - 8S_3$   
 e)  $S_1S_2 - 3S_3$  k)  $S_1^3 - 3S_1S_2 + 3S_3$   
 f)  $S_1S_2 - 3S_3$  l)  $S_2S_3 - 3S_1S_4$
- 2 a)  $f_1^3 - 6f_1^2 + 9f_1 - 3f_1f_2 + 3f_2 - 4$   
 b)  $-\frac{1}{2}f_1^3 + 3f_1f_2/2$   
 c)  $\frac{1}{2}f_1^3 - \frac{1}{2}f_1f_2 - 3f_3$   
 d)  $f_1^3 + 3f_1^2 - 3f_1f_2 + 3f_3 - 3f_2$   
 e)  $(f_1f_2 + f_2 - f_3)/3$   
 f)  $f_1^4 - 4f_1^3 - 16f_1^2 + 2f_1^2f_2 - 2f_1$   
 $- 2f_1f_2 - 2f_1f_3 + f_2^2 - 10f_2 - 6f_3 + 2f_4$

CHAPTER 12

- 3— 2 a) -14 b) 9 c) 0  
 3 a) -3 b) 0 c) 16
- 7— 1 a) 1 d) -6 g)  $-9i$  j) 8 m) 4  
 b) 37 e) 0 h) 0 k) 35 n) 0  
 c) 0 f) 0 i) 1 l) -3 o) -16
- 3 a)  $x = 1, 2, 3$  b)  $x = 0$  c)  $x = 0$
- 9— 1 a) Three b) Two c) Two d) Two e) Two  
 2 a) One if  $x = 1$ , two if  $x = -2$ , otherwise three  
 b) Three for all  $x$   
 c) Two if  $x = -1, -2$ ; otherwise three  
 3 Three if no two of  $a, b, c$  are equal, two if exactly two of  $a, b, c$  are equal; one if all three are equal

CHAPTER 13

- 1— 3 a)  $c_1 = 2, c_2 = -1, c_3 = 1$  e)  $c_1 = 1, c_2 = -1, c_3 = i$   
 b)  $c_1 = 2, c_2 = 2, c_3 = -1$  f) Independent  
 c)  $c_1 = -1, c_2 = 2, c_3 = -1$  g) Independent  
 d) Independent
- 4 a)  $k = 1; c_1 = 1, c_2 = -1, c_3 = 0$   
 b)  $k = 0; c_1 = 2, c_2 = 2, c_3 = -1$   
 c) None  
 d) All;  $c_1 = -5k, c_2 = k, c_3 = -3k, c_4 = 2k + 8$   
 e)  $k = 1; c_1 = 1, c_2 = 1, c_3 = -1$   
 f) None

## Sect. Ex.

2— 1 a)  $c_1 = -1, c_2 = 1, c_3 = 1$

b)  $c_1 = -4, c_2 = 3, c_3 = 1$

c)  $c_1 = 2, c_2 = -3, c_3 = 1$

d)  $c_1 = 2, c_2 = 2, c_3 = -1, c_4 = -1$

e)  $c_1 = 2, c_2 = 2, c_3 = 0, c_4 = -1$

3 a)  $k = 0, c_1 = 1, c_2 = -1, c_3 = 0$ ; or  $k = 1, c_1 = 1, c_2 = 0, c_3 = -1$

b)  $k = 1, c_1 = 1, c_2 = -1, c_3 = 0$ ; or  $k = 2, c_1 = 0, c_2 = 2, c_3 = -1$

c)  $k = -2, c_1 = 0, c_2 = 1, c_3 = -1$

d)  $k = 0, c_1 = 0, c_2 = 1, c_3 = -1$ ; or  $k = -1, c_1 = 1, c_2 = -1, c_3 = 0$

e)  $k = 0, c_1 = 0, c_2 = 1, c_3 = 1$

f) None

g) All,  $c_1 = 2, c_2 = -1, c_3 = 1$

h)  $k = 1, c_1 = 2, c_2 = 3, c_3 = -1$

i) All,  $c_1 = 1, c_2 = k + 1, c_3 = -k$

4— 1 a)  $(-1\frac{1}{2}, 4, -3\frac{1}{2})$  d)  $(7\frac{1}{4}, 13\frac{3}{4}, 6, 3\frac{1}{4})$

b)  $(-1\frac{1}{2}, -5\frac{1}{2}, -1)$  e)  $(6\frac{3}{4}, -2\frac{3}{4}, -2\frac{1}{4}, -11\frac{5}{4})$

c)  $(60\frac{1}{4}, 7\frac{1}{4}, 45\frac{1}{4})$

2  $(13\frac{1}{3}, 31\frac{1}{6}, 16\frac{1}{3})$

6— 1 a)  $x = 3 + 10z, y = 2 + 8z$

b)  $y = \frac{1}{2}(1 - 3x), z = 0$

c) Inconsistent

d) Inconsistent

e)  $x = (1 - 3z)/5, y = (z - 3)/5, w = -9z$

f)  $x = 5z - 8w + 2, y = 7z - 11w$

2 a)  $x = 0, y = 0, z = 0$  c)  $y = x, z = x, w = -4x$

b)  $x = -13y, z = 12y$  f)  $x = 2z/5, y = 11z/10, w = 3z/2$

c)  $x = -z, y = 0, w = 0$  g)  $x = 0, y = z, w = z$

d)  $x = w, y = 0, z = 0$

3 a)  $k = 0, x = 6z/7, y = 8z/7$

b)  $k = 2, x = (1 - 5z)/3, y = (z - 2)/3; k = -1,$

$x = (1 - 2z)/3, y = -(5z + 2)/3; \text{ all other } k, x = \frac{1}{2}, y = -\frac{2}{3}, z = 0$

c)  $k = 1, y = \frac{1}{2}(3x - 2), z = \frac{1}{2}(4 - 5x)$

d)  $k = 1, x = -1, y = 1$

e)  $k = 1, x = w - 2, y = w - 3, z = w; k = 2, x = w - 2, y = w - 6, z = w$

f)  $k = 1, x = -5y + 5z + 2, w = 13y - 14z - 2; k \neq 1, x = \frac{1}{2}(k - 6)(z + 4) - 18, y = 3(z + 4)/2, w = \frac{1}{2}(12 - k)(z + 4) + 54$



Sect Er

g) Inconsistent for all  $k$

$$h) k \neq 2, x = \frac{(32k - 77k)}{42(k - 2)} + \frac{2w}{3}, y = \frac{(2k^2 + 7k)}{42(k - 2)} - \frac{w}{3}$$

$$z = \frac{k}{7(k - 2)}$$

4 a)  $k = 2, x = -z/2, y = z/8; k = 2, x = -z/6, y = 3z/8$

b) None

c)  $k = 1, x = -y, z = -y, w = y; k = -1, x = y, z = y, w = y;$   
 $k = i, x = -iy, z = iy, w = -y; k = -i, x = iy, z = -iy,$   
 $w = -y$

d)  $k = 0, z = -x, w = -y; k = -1, z = y, w = x; \text{all other } k,$   
 $y = -x, z = -x, w = x$

e)  $k = 3, y = 2x, z = 0, w = -2x/3; k = 0, x = y = z = 0, w$   
 arbitrary

f)  $k = -5, x = -3/5, y = 6z/5$

5  $y = 2x, z = 0$  and  $x = z, y = 3z$

6  $x = -z, y = 2z$

7  $a = 0, b = -1$

7 - 1 a) Independent

b)  $c_1 = 1, c_2 = -1, c_3 = -1$

c) Independent

d) Independent

e)  $c_1 = 2, c_2 = -1, c_3 = -1$

f)  $a \neq n$ , independent;  $a = n, c_1 = 1, c_2 = -1, c_3 = 2n$

g)  $n \neq 3$ , independent,  $n = 3, c_1 = -2, c_2 = 1, c_3 = 1$

# CHAPTER 14

2 a)  $a = 1, x = -1; a = -1, x =$

b)  $a = 0, x = 0$

c)  $a = 0, x = 1; a = 1, x = -2$

d)  $a = 0, b$  arbitrary,  $x = \frac{1}{2}(-b + \sqrt{b^2 - 4})$

e)  $a + b + 1 = 0, x = 1; 2a - b + 1 = 0, x = -2$

f)  $c^3 - acd^2 + a^2c + b^2c - abdc - bcd + ad^2 - 2arc + bd^2e$   
 $- 2bc^2 - cd^3 + 3cde + c^2 = 0$

g)  $a = -1, x = 0, 1$

4 - 1 a)  $x = -2$  c) None

i) None

b)  $x = 1$  f)  $x = \frac{1}{2}(-1 \pm i\sqrt{3})$  j)  $x = i$

c) None g) The roots of  $x^3 + x + 1$  k)  $x = \frac{1}{2}(3 \pm i\sqrt{11})$

d)  $x = +1$  h)  $x = \pm i$

2 a) One for  $a = 0$   $\pm \frac{1}{\sqrt{2}}$

*Sect. Ex.*

- b) One for  $a = -\frac{1}{2}$ , two for  $a = 0$   
 c) One for  $a = -\frac{1}{2}$ , two for  $a = 0$   
 d) None  
 e) Three for  $a = 2$   
 f) One for  $a = 0$ , three for  $a = -2$   
 g) One for  $2a + b = 0$ ,  $a \neq 0$ ; two for  $a + b = 0$ ,  $a \neq 0$ ; three for  $a = b = 0$   
 h) Two for  $b = 0$ ,  $a = 0, -1$ ; one for  $b = 0$ ,  $a \neq 0$ ,  $-1$ ; one for  $b \neq 0$ ,  $a + b + 1 = 0$   
 i) Two for every value of  $a$   
 j) One for  $a = 0$ ,  $\frac{1}{2}(-5 \pm i\sqrt{3})$   
 k) Three for  $a = 0$ ; one for  $b = 0$ ,  $a \neq 0$ ,  $-1$ ; two for  $b = 0$ ,  $a = -1$ ; one for  $a + b + 1 = 0$ ;  $a \neq 0$ ,  $b \neq 0$   
 l) One for  $a = -\frac{3}{2}$   
 m) Two for  $a = 2$   
 n) Two for  $a = 0, 2$ , one for  $a = -4$   
 o) One for  $a = -1$ ,  $-\frac{1}{3}$ ; three for  $a = 0$   
 p) One for  $a = 1$ ,  $b = -3$   
 q) One for  $a = b = -2$
- 3 a)  $0, -\frac{1}{4}$       b)  $0, 1$       c)  $0, 1, \frac{1}{2}(-1 \pm i\sqrt{3})$
- 5 a)  $(1, 2), (4, 2)$   
 b)  $(1, 1), (-1, -1), (\pm\sqrt{5}, 0)$   
 c)  $(\frac{i}{\sqrt{2}}, -\frac{i}{\sqrt{2}}), (-\frac{i}{\sqrt{2}}, \frac{i}{\sqrt{2}})$   
 d) None  
 e)  $(0, 0), (2, -4), (3, 4)$   
 f)  $(1 + \frac{1}{y}, y)$  for all  $y \neq 0$   
 g)  $(1, 0), (0, i), (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), (-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$   
 h)  $(0, -1), (-1, -\frac{1}{2}), (1, y)$  for all  $y$   
 i)  $(0, 0)$   
 j)  $(-2, a)$  if  $a \neq 0$ ,  $(x, 0)$  for all  $x$  if  $a = 0$   
 k)  $(-\frac{1}{2}a, \frac{5a}{2}), (\frac{a}{2}, -\frac{5a}{2})$  if  $a \neq 0$ ;  $(x, -x)$  for all  $x$  if  $a = 0$   
 l)  $(-\frac{2}{a+b}, b), (-\frac{1}{a}, a)$  if  $a + b \neq 0$ ,  $a \neq 0$ ;  $(-\frac{2}{b}, b)$  if  $a = 0$ ,  $b \neq 0$ ;  $(-\frac{1}{a}, a)$  if  $a + b = 0$ ,  $a \neq 0$ ; none if  $a = b = 0$   
 m)  $(0, 0), (a/2, a/2)$  if  $a \neq 0$ ;  $(x, -x)$  for all  $x$  if  $a = 0$
- 6—1 a)  $2x - y + 1; (-\frac{5}{6}, \frac{3}{8}), (x, 2x + 1)$  for all  $x$   
 b) None;  $(0, 0), (2, 2), (-2, 2), (-\frac{1}{2}, \frac{1}{2}), (-2, -1)$

Sect. Ex.

c)  $x - y$ ; (1, 3), (-1, 3), (x, x) for all  $x$

d)  $y + 2$ ; (x, -2) for all  $x$

2 a)  $a = 1, x^2 - y^2$

e)  $a = 0, x + y; a = 1,$

b)  $a = 0, x - y; a = -1, (x - y)^2 - 1$

$(x + y)(x + y - 1);$

c)  $a = 1, y - 1$

$a = -1, x + y + 1$

d) None

f) All  $a, x - y + a$

3 a) -1

c) 0

e) All  $a$

g) 0, 2, -2

b) 0, 1

d)  $1, \frac{3}{2}$

f) No  $a$

7

a)  $(0, \pm \sqrt{2}, 1)$

b)  $(\pm 3, \pm 2, \pm 1)$

c)  $(2, 1, 1), (-2, -1, -1), (-i\sqrt{2}, i\sqrt{2}, i\sqrt{2}), (i\sqrt{2}, -i\sqrt{2}, -i\sqrt{2})$

d)  $(0, 0, 0), (1, 1, 1), (-1, 1, -1), (1, -1, -1), (-1, -1, 1)$

e) Inconsistent

f)  $(-1/2, -1/2, -1/4)$

g)  $(x, 1 - x, x^2 - x + 1)$  for all  $x$



# I N D E X

*Numbers refer to pages*

## A

Absolute value, 9, 37  
 Addition of complex numbers, 2, 3, 8-9  
 Addition of polynomials, 16, 54-55, 171, 175, 180  
 Adjoint, 205  
 Adjunction of algebraic numbers, 160-163  
 Adjunction of radicals, 164-166  
 Adjunction to a field, 159, 160-166  
 Algebra, fundamental theorem of, 39  
 Algebraic extension, 157-158, 162, 164  
 Algebraic number, 152, 258  
 Algebraic number over a field, 153-154, 157, 158  
     degree of, 153, 155, 157-158, 160, 162, 163, 164-168  
 Algebraic numbers, adjunction of, 160-163  
 Algorithm, division  
     *See* Division algorithm  
 Algorithm, Euclidean  
     *See* Euclidean algorithm  
 Amplitude of complex number, 10, 11  
 Angle trisection, 138, 142, 144, 149-151  
 Approximation to real roots, 103-113  
     by location principle, 104-105  
     graphical, 103-104  
     Horner's method of, 105-106  
     Newton's method of, 108-111  
 Associate of integer, 37  
     of polynomial, 26-29, 31, 32, 33, 34, 35  
 Associated homogeneous system, 234-235  
 Associative laws, 2, 3  
 Augmented matrix, 225  
 Axis, imaginary, 7  
     real, 7

## B

Basis of extension of field, 155, 158, 160, 162, 163  
 Biquadratic polynomial, 16  
 Budan sequence, 85-87  
 Budan's theorem, 87-91

## C

Cancellation law, 19, 176  
 Cardan's solution of cubic, 115-119  
 Circle squaring, 152  
 Closure laws, 2  
 Coefficient, 15, 171  
     leading, 15, 55  
 Coefficients, relations of to roots, 44-46  
 Cofactor, 196, 197, 203  
 Column of determinant, 191  
     expansion by, 197  
 Column of matrix, 191, 207  
 Columns, interchange of, 198-199  
     interchange of rows and, 197  
 Common factor, highest  
     *See* Highest common factor  
 Common factor of polynomials, 27, 31, 241, 243-244, 253-255, 257  
 Common roots, 51, 52, 64-65, 240, 241, 244-247, 250  
 Commutative laws, 2  
 Complement, 195  
 Complex number(s), 2  
     addition of, 2, 3, 8, 9  
     amplitude of, 10, 11  
     associative laws for, 2, 3  
     closure laws for, 2  
     commutative laws for, 2  
     conjugate of, 6  
     de Moivre's theorem for, 10  
     difference of, 2, 9  
     distributive law for, 3

Complex number(s), division of, 3, 8, 11  
 geometrical representation of, 7  
 imaginary, 5  
 modulus of, 7-9  
 multiplication of, 2-3  
 negative of, 2, 4, 9  
 polar form of, 10, 11  
 powers of, 10  
 product of, 2, 7, 10  
 product law for, 3  
 pure imaginary, 5, 7  
 quotient of, 3, 8, 11  
 rational operations on, 3, 21  
 real, 4, 5, 7, 11  
 reciprocal of, 3  
 roots of, 12-13  
 subtraction of, 2, 9  
 sum of, 2, 8-9  
 trigonometric form of, 10, 11  
 un\*x, 3  
 zero, 2, 9, 18

Composite function formula, 56

Composite polynomial, 31-32

Configuration, numbers of, 134

Conjugate complex roots, 65

Conjugate of complex number, 6

Conjugate square roots, 70-71

Consecutive roots, 76, 77, 78, 79

Consistent linear equations, 225-228, 231, 234

Consistent over a field, 239

Constant polynomial, 16, 171

term, 15

Constants, linear dependence of, 213-217, 236  
 linear independence of, 213

Constructibility, 132-137

Construction of regular polygons, 142, 144, 151-152

Continuous function, 21

Coordinates of point, 7, 134

Correspondence, one-to-one, 7

Cramer's rule, 221-224

Cube, duplication of, 143

Cubic, discriminant of, 122-124, 125  
 polynomial, 16  
 reduced, 115-116, 118, 123  
 resolvent, 128, 130, 131  
 solution of, 115-119  
 solvability of by square roots, 140-141  
 trigonometric solution of, 126-127

## D

Decreasing, monotonically, 79, 81, 82

Degree in a variable, 174, 181

Degree of algebraic number, 153, 155, 157-158, 160, 162, 163, 164-168  
 of field, 155-157, 158, 159, 160-162, 163, 164, 166  
 of polynomial, 16, 18, 19, 171, 174, 176-177  
 of term, 171

De Moivre's theorem, 10

Dependence, linear  
*See* Linear dependence

Dependent, linearly  
*See* Linear dependence

Derivative of determinant, 203-204

Derivative of polynomial, 54-56

Descartes' rule, 93

Determinant, 191, 238, 239  
 adjoint of, 205  
 cofactor of element of, 196, 197, 203  
 column of, 191  
 complement of element of, 195  
 derivative of, 203-204  
 element of, 191  
 expansion of, 192-193, 194, 195-196, 197  
 expansion of by columns, 197  
 expansion of by rows, 195-196  
 interchange of columns of, 198-199  
 interchange of rows of, 198-199  
 interchange of rows and columns of, 197  
 main diagonal of, 191  
 of linear equations, 221  
 of matrix, 191, 207  
 order of, 191  
 orthogonal, 206  
 row of, 191  
 term of, 192  
 transpose of, 197-198

Determinants, product of, 204-205

Diagonal, main, of determinant, 194

Difference of complex numbers, 2, 9  
 of polynomials, 16, 171, 175

Differentiate, 54

Discriminant, 122

Discriminant of cubic, 122, 124, 125  
 of quartic, 130, 131

Distributive law, 3

Divisibility of integers, 37  
of polynomials, 26  
Division, synthetic, 41-42  
Division algorithm for integers, 36  
for polynomials, 23-24  
quotient in, 24  
remainder in, 24, 26  
Division of complex numbers, 3, 8, 11  
Divisor of polynomial, 26  
Domain of rationality, 22  
Double root, 40  
Duplication of cube, 143

## E

Element of determinant, 191  
of matrix, 191  
Elementary symmetric polynomials,  
178-179, 181, 182  
Eliminant, 242  
Elimination, 210  
Laurent's method of, 250  
successive, 258  
Sylvester's method of, 242, 247  
Equation, final, 251, 253  
Equation, root of, 17  
Equations, linear, 219-220  
Equations, simultaneous, solution of  
220, 251, 257, 260  
Euclidean algorithm for integers, 37  
for polynomials, 27-28, 241  
Expansion, Taylor, 61-63  
Expansion of determinant  
*See* Determinant  
Expansion of polynomial, 21, 60-63  
Extension of field, 155  
algebraic, 157-158, 162, 164  
basis of, 155, 158, 160, 162, 163  
degree of, 155-157, 158, 159, 160-  
162, 163, 164, 166

## F

Factor, common, of polynomials, 27,  
31, 241, 243-244, 253-255, 257  
Factor, highest common  
*See* Highest common factor  
Factor of polynomial, 26  
Factor theorem, 17, 25, 39  
Factorization of integers, 37, 38  
of polynomials, 33-35, 40, 44, 60,  
65-66, 128, 258

Ferrari's solution of quartic, 128  
Field, 22, 153, 159  
adjunction to  $a$ , 159, 160-166  
algebraic extension of, 157-158, 162,  
164  
algebraic over  $a$ , 153, 157, 158  
basis of, 153, 158, 160, 162, 163  
consistent over  $a$ , 239  
degree of algebraic number over  $a$ ,  
153, 155, 157-158, 160, 162, 163,  
164, 168  
degree of extension of, 155-157,  
158, 159, 160-162, 163, 164, 166  
extension of, 155  
field algebraic over  $a$ , 157-158, 162,  
164  
linear dependence over  $a$ , 156-157,  
158, 238, 239  
linear independence over  $a$ , 156  
minimum polynomial over  $a$ , 153-  
154, 155  
transcendental over  $a$ , 153, 155  
Figure, numbers of  $a$ , 134  
Final equation, 251, 253  
Function, 15, 170  
continuous, 21  
Function of function formula, 56  
Fundamental theorem of algebra, 39  
on symmetric polynomials, 182-  
181

## G

Geometrical representation of com-  
plex numbers, 7  
Graph of polynomial, 83-84  
Graphical approximation, 103-104

## H

H.C.F., 27  
Highest common factor of integers,  
37  
of polynomials, 27-29, 30, 51, 57-58,  
258  
Homogeneous linear equations, 231-  
232  
Homogeneous polynomial, 174, 176,  
177, 178, 181, 185  
Homogeneous system, associated,  
234-235  
Horner's method, 105-106

## I

- Identical polynomials, 171
- Identically, vanishing, 16, 18, 171, 172-173
- Identity sign, 15
- Imaginary axis, 7
  - number, 5
  - pure, 5, 7
  - unit, 5
- Inconsistent linear equations, 225
- Increasing, monotonically, 79, 81, 82
- Indecomposable polynomial, 32
- Independence, linear
  - See* Linear independence
- Independent, linearly
  - See* Linear independence
- Induction, mathematical, 261-264
- Integer, associate of, 37
  - divisible by, 37
  - prime, 37, 38
- Integers, division algorithm for, 36
  - Euclidean algorithm for, 37
  - factorization of, 37, 38
  - highest common factor of, 37
  - relatively prime, 37
- Interchange of columns, 198-199
  - of rows and columns, 197
- Interpolation, Newton's formula for, 21
- Interval, 79
- Interval, roots in an, 87, 88, 96, 98
- Inversion, 194
- Irrational number, 1
- Irreducible polynomial, 32, 33, 39, 53, 64, 65-66, 70, 161, 177, 178, 181, 257

## L

- Laurent's method of elimination, 250
- Leading coefficient, 15, 55
- L'Hospital's rule, 56
- Line, 132, 134
- Linear dependence of constants, 213-217, 236
  - of polynomials, 235-237, 238, 243-244
  - over a field, 156-157, 158, 238, 239
- Linear equations, 219-220
  - associated homogeneous system of, 234-235

- Linear equations, augmented matrix of, 225
  - consistent, 225-228, 231, 234
  - consistent over a field, 239
  - Cramer's rule for, 221-224
  - determinant of, 221
  - homogeneous, 231, 232
  - inconsistent, 225
  - matrix of, 225, 228
  - non-homogeneous, 231
  - solution of, 220, 234
  - trivial solution of, 231
- Linear independence of constants, 213
  - of polynomials, 235, 237
  - over a field, 156, 158
- Linear polynomial, 16, 17, 34, 39
- Linearly dependent
  - See* Linear dependence
- Linearly independent
  - See* Linear independence
- Location principle, 73-74, 104-105

## M

- Main diagonal of determinant, 194
- Mathematical induction, 261-264
- Matrices, product of, 211
- Matrix, 190, 191, 206-207
  - augmented, 225
  - column of, 191, 207
  - determinant of, 191, 207
  - element of, 191
  - $m$  by  $n$ , 206-207
  - minor of, 207
  - $n$ -rowed, 190
  - of linear equations, 225, 228
  - order of, 190
  - rank of, 207-208, 209, 210, 216, 239
  - row of, 191, 207
  - square, 190
  - $m$  by  $n$  matrix, 206-207
- Mean, theorem of the, 80
- Mean-value theorem, 80
- Minimum polynomial, 153-154, 155
- Minor of matrix, 207
- Modulus of complex number, 7-9
- Monotonically decreasing, 79, 81, 82
  - increasing, 79, 81, 82
- Multiple root, 40, 57, 100, 122
- Multiple square root, order of, 138-139, 146



Multiplication of complex numbers,  
 2-3, 7, 10  
 of determinants, 204-205  
 of matrices, 211  
 of polynomials, 16, 55, 171, 175-177,  
 180  
 Multiplicity of root, 40, 56-58, 60

# N

Negative of complex number, 2, 4, 9  
 Negative roots, 94  
 Newton's interpolation formula, 21  
 method of approximation, 108-111  
 Non-homogeneous linear system, 231  
 $n$ -rowed square matrix, 190  
 $n$ th root, 12  
 Number, algebraic, 152, 254  
 algebraic over a field, 153-154, 157,  
 158  
 complex, 2  
 imaginary, 5  
 irrational, 1  
 pure imaginary, 5, 7  
 rational, 1, 23, 37  
 real, 1, 5  
 real complex, 4, 5, 7, 11  
 transcendental, 152  
 transcendental over a field, 153, 155  
 Numbers of a configuration, 134  
 of a figure, 134

# O

Obtainable by radicals, 166-168  
 by rational operations and . . . , 134  
 135, 137, 139, 140-141, 143, 144,  
 146-148, 149, 163  
 One-to-one correspondence, 7  
 Operations, rational, 3, 21  
 Order of determinant, 191  
 of matrix, 190  
 of multiple square root, 138-139, 146  
 of root, 40  
 Ordered pair, 2  
 Orthogonal determinant, 206

# P

Pair, ordered, 2  
 Periodic, 20  
 Point, coordinates of, 7, 134

Polar form of complex number, 10, 11  
 Polygons, regular, 142, 144, 151-152  
 Polynomial(s), 15-16, 170-171  
 addition of, 16, 54-55, 171, 175, 180  
 associate of, 26, 29, 31, 32, 33, 34, 35  
 Budan's theorem for, 87-91  
 cancellation law for, 19, 176  
 coefficient of, 15, 171  
 coefficient of, leading, 15, 55  
 common factors of, 27, 31, 241, 243-  
 244, 253-255, 257  
 common roots of, 51, 52, 64-65, 240,  
 241, 244-247, 250  
 composite, 31, 32  
 consecutive roots of, 76, 77, 78, 79  
 constant, 16, 171  
 constant term of, 15  
 cubic, 16  
 decreasing, monotonically, 79, 81,  
 82  
 degree of, 16, 18, 19, 171, 174, 176-  
 177  
 degree of in a variable, 174, 181  
 degree of term of, 171  
 derivative of, 54-56  
 Descartes' rule for, 93  
 difference of, 16, 171, 175  
 discriminant of, 122  
 divisibility of, 26  
 division algorithm for, 23-24  
 divisor of, 26  
 double root of, 40  
 elementary symmetric, 178-179,  
 181, 182  
 Euclidean algorithm for, 27-28, 241  
 expansion of, 21, 60-63  
 expansion of, Taylor, 61-63  
 factor of, 26  
 factor theorem for, 17, 25, 39  
 factorization of, 33-35, 40, 44, 60,  
 65-66, 128, 258  
 fundamental theorem on symmetric,  
 182-184  
 graph of, 82-84  
 highest common factor of, 27-29,  
 30, 51, 57-58, 253  
 homogeneous, 174, 176, 177, 178,  
 181, 185  
 identical, 171  
 identically vanishing, 16, 18, 171,  
 172-173  
 increasing, monotonically, 79, 81, 82

**Polynomial(s)**, indecomposable, 32  
 irreducible, 32, 33, 39, 53, 64, 65-66, 70, 161, 177, 178, 181, 257  
 leading coefficient of, 15, 55  
 linear, 16, 34, 39, 171  
 linearly dependent, 235-237, 238, 243-244  
 linearly independent, 235, 237  
 location principle for, 73-74, 104-105  
 mean-value theorem for, 80  
 minimum, 153, 154, 155  
 monotonically decreasing, 79, 81, 82  
 monotonically increasing, 79, 81, 82  
 multiple root of, 40, 57, 100, 122  
 multiplicity of root of, 40-41, 56-58, 60  
 order of root of, 40  
 prime, 32, 33  
 prime to each other, 30-31, 33  
 product of, 16, 55, 171, 175, 177, 180  
 properties of symmetric, 179, 181  
 quadratic, 16, 171  
 quartic, 16  
 quintic, 16  
 rational roots of, 67  
 reducible, 31, 32, 33, 34, 39-40, 64, 65, 177, 236  
 relations among roots and coefficients of, 44-46  
 relatively prime, 30, 31, 33  
 remainder theorem for, 25  
 Rolle's theorem for, 78, 79, 82  
 root of, 16, 17, 18, 40  
 sign of for large  $x$ , 74, 75  
 simple root of, 40  
 Sturm's theorem for, 98-99  
 sum of, 16, 51, 55, 171, 175, 180  
 symmetric, 178, 187  
 symmetric, elementary, 178-179, 181, 182  
 Taylor expansion of, 61-63  
 term of, 171  
 the roots of, 40-41  
 transformation of roots of, 48-49, 50, 63  
 triple root of, 40  
 unique factorization of, 33-35, 40, 44, 60, 65-66, 258  
 unique representation of, 19, 21, 173-174

**Polynomial(s)**, vanishing identically, 16, 18, 171, 172-173  
 vanishing of, 16-17  
 weight of term of, 186  
 zero, 16, 54, 171  
 zero of, 16  
**Positive roots**, 93, 95, 96  
**Powers of complex numbers**, 10  
**Prime integer**, 37, 38  
 polynomial, 32, 33, 171  
 Prime to each other, 30-31, 33  
**Product law for complex numbers**, 3  
**Product of complex numbers**, 2, 7, 10  
 of determinants, 204-205  
 of matrices, 211  
 of polynomials, 16, 55, 171, 175, 177, 180  
**Pure imaginary number**, 5, 7

## Q

**Quadratic polynomial**, 16, 171  
**Quartic polynomial**, 16  
 discriminant of, 130, 131  
 reduced, 129  
 resolvent cubic of, 128, 130, 131  
 solution of, 128  
 solvability of by square roots, 146, 148  
**Quintic polynomial**, 16  
**Quotient in division algorithm**, 24  
**Quotient of complex numbers**, 3, 8, 11

## R

**Radicals**, adjunction of, 164, 166  
 obtainable by, 166, 168  
 solvable by, 114-115, 168  
**Rank of matrix**, 207-208, 209, 210, 216, 239  
**Rational in  $a_1, a_2, \dots$** , 135, 137, 139, 140-141, 143, 144, 146-148  
**Rational number**, 1, 23, 37  
**Rational operations**, 3, 21  
 obtainable by  $\dots$ , 134-135, 137, 139, 140, 141, 143, 144, 149  
**Rational roots**, 67  
**Rationality**, domain of, 22  
**Ray**, 132, 134  
**Real axis**, 7  
**Real complex number**, 4, 5, 7, 11  
**Real number**, 1, 5  
**Real roots**, 94, 95, 101

Reciprocal of complex number, 3  
 Reduced cubic, 115-116, 118, 123  
     quartic, 129  
 Reducible polynomial, 31-32, 33, 34,  
     39 40, 64, 65, 177, 256  
 Regular polygons, 142, 141, 151-152  
 Relations among roots and coeffi-  
     cients, 44 46  
 Relatively prime integers, 37  
     polynomials, 30 31, 33  
 Remainder in division algorithm, 24,  
     26  
 Remainder theorem, 25  
 Representation, geometrical, of com-  
     plex numbers, 7  
     unique, of polynomial, 19, 21, 173-  
     174  
 Resolvent cubic, 128, 130, 131  
 Resultant, 242  
     Sylvester, 248, 250  
 Rolle's theorem, 78, 79, 82  
 Root of equation, 17  
 Roots of complex numbers, 12-13  
 Root(s) of polynomials, 16, 17, 18, 39,  
     40  
     approximations to, 103-113  
     common, 51, 52, 64 65, 240, 241,  
         244 247, 250  
     conjugate complex, 65  
     consecutive, 76, 77, 78, 79  
     double, 40  
     exceeding a given number, 92 93,  
         101  
     in an interval, 87 88, 96, 98  
      $m$ -fold, 40  
     multiple, 40, 57, 100, 122  
     multiplicity of, 40, 56 58, 60  
     negative, 94  
     number of, 41, 87-88, 91, 98, 101,  
         102  
     order of, 40  
     positive, 93, 95, 96  
     rational, 67  
     real, 94, 95, 101  
     relations among and coefficients,  
         44-46  
     simple, 40  
     the, 40 41  
     transformations of the, 48-49, 50,  
         63  
     triple, 40  
 Roots of unity, 12-13, 14, 38, 165

Row of determinant, 191  
     expansion by, 195-196  
 Row of matrix, 191, 207  
 Rows, interchange of, 198-199  
 Rows, interchange of and columns, 197  
 Ruler and compass constructibility,  
     132-137

## S

Segment, 132, 134  
 Sequence, Budan, 85-87  
     Sturm, 96-97  
 Sign, variations in, 85, 92  
 Sign of polynomial for large  $x$ , 74-75  
 Simple root, 40  
 Simultaneous equations, linear, 219  
 Simultaneous equations, solution of,  
     220, 251, 257, 260  
 Solution, trivial, 231  
 Solution of cubic, 115-119  
     of linear equations, 220, 234  
     of quartic, 128  
     of simultaneous equations, 220, 251,  
         257, 260  
 Solvable by radicals, 114-115, 165  
 Square matrix, 190  
 Square root of order  $n$ , 138-139, 146  
 Square roots, conjugate, 70-71  
 Squaring circle, 152  
 Sturm sequence, 96-97  
 Sturm's theorem, 98-99  
 Subtraction of complex numbers, 2, 9  
     of polynomials, 16, 171, 175  
 Successive elimination, 258  
 Sum of complex numbers, 2, 8-9  
     of polynomials, 16, 54-55, 171, 175,  
         180  
 Sylvester resultant, 248, 250  
 Sylvester's method of elimination,  
     242, 247  
 Symmetric polynomials, 178-187  
     elementary, 178 179, 181, 182  
     fundamental theorem on, 182-184  
     properties of, 179 181  
 Synthetic division, 41-42

## T

Taylor expansion, 61-63  
 Teym, constant, 15  
     degree of, 171

Term of determinant, 192  
 of polynomial, 171  
 weight of, 186  
 The roots of a polynomial, 40-41  
 Theorem of the mean, 80  
 Transcendental number, 152  
 Transcendental over a field, 153, 155  
 Transformations of roots, 48-49, 50, 63  
 Transpose of determinant, 197-198  
 Trigonometric form of complex number, 10, 11  
 Trigonometric solution of cubic, 126, 127  
 Triple root, 40  
 Trisection of angle, 138, 142, 144, 149, 151  
 Trivial solution, 231

## U

Unique factorization of integers, 37  
 of polynomials, 33-35, 40, 44, 60, 65-66, 258

Unique representation of polynomial, 19, 21, 173-174  
 Unit, imaginary, 5  
 Unity, roots of, 12-13, 14, 38, 165  
 Unity complex number, 3

## V

Value, absolute, 9, 37  
 Vanishing identically, 16, 18, 171, 172-173  
 Vanishing of polynomial, 16-17  
 Variations in sign, 85, 92

## W

Weight of term, 186  
 Wronskian, 238

## Z

Zero complex number, 2, 9  
 polynomial, 16, 18, 54, 171  
 Zero of polynomial, 16